PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084271
(43)Date of publication of application : 22.03.2002

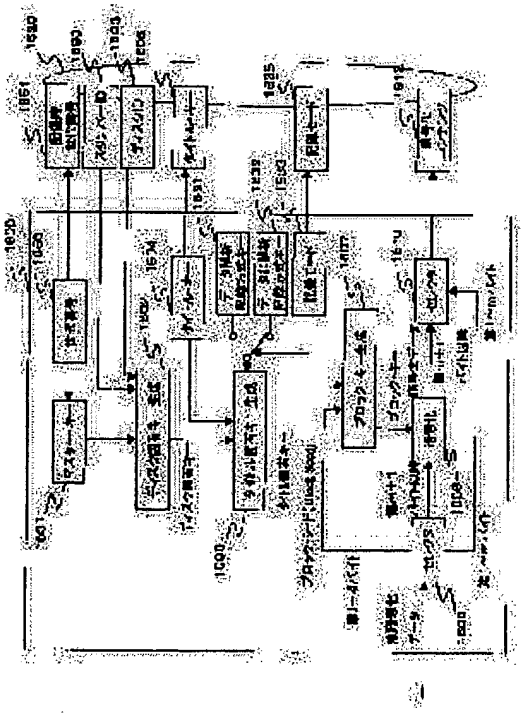
(51)Int.Cl. H04L 9/08
G11B 20/10

(21)Application number : 2000-270919
(22)Date of filing : 07.09.2000

(71)Applicant : SONY CORP
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO

(54) INFORMATION RECORDING APPARATUS, INFORMATION REPRODUCING DEVICE, INFORMATION RECORDING METHOD, INFORMATION REPRODUCING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information recording apparatus and reproducing devices that can effectively exclude utilization of illegal contents.
SOLUTION: The recording medium of this invention stores secret information whose write/read method is difficult for its analysis and that can be read only by a special read method, and the secrete information is used for an encryption key for encryption or decoding processing of contents in recording or reproducing contents such as music data image data to/from the recording medium. The secret information is e.g. a stamper ID, and the stamper ID as the secrete information, a master key and a medium key or the like distributed through key distribution configuration of a tree structure are used to generate an encryption processing key for contents. Thus, a special read method as to the secret information can be performed and only a legal device to which the key is distributed through the key distribution configuration of a tree structure can utilize contents.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－84271
（P2002－84271A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６０１Ｄ　５Ｊ１０４

審査請求　未請求　請求項の数40　ＯＬ　（全 56 頁）

(21)出願番号　特願2000－270919(P2000－270919)

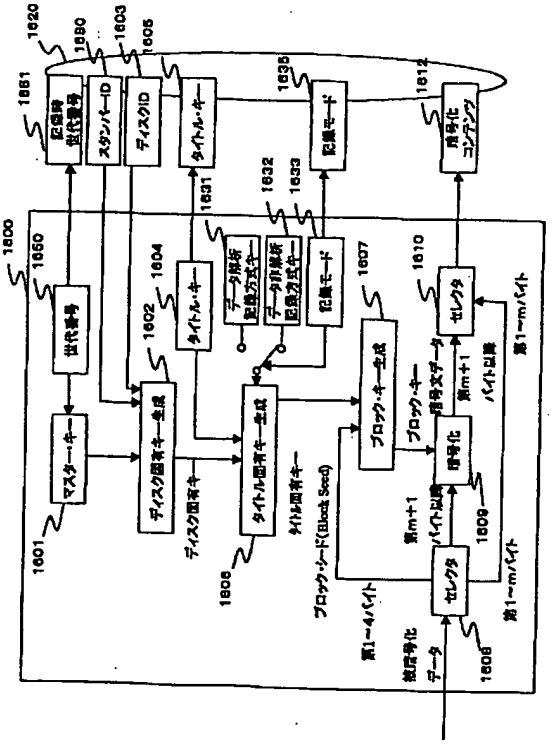
(22)出願日　平成12年９月７日(2000.9.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】
【課題】　不正なコンテンツの利用を効果的に排除可能とした情報記録、再生装置を提供する。
【解決手段】　記録媒体に、あらかじめその書き込み／読出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報を格納し、記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記秘密情報を作用させる。秘密情報は、例えばスタンパーＩＤであり、秘密情報としてのスタンパーＩＤと、ツリー構造の鍵配布構成により配布されるマスターキー、メディアキー等と共にコンテンツの暗号処理鍵の生成を行なう。従って、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。



1

【特許請求の範囲】

【請求項１】記録媒体に情報を記録する情報記録装置において、

記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する構成を有することを特徴とする情報記録装置。

【請求項２】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、

前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項３】前記暗号処理手段は、

前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能な構成としたことを特徴とする請求項１に記載の情報記録装置。

【請求項４】前記情報記録装置は、さらに、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成する構成であり、

前記暗号化キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータとして構成されていることを特徴とする請求項１に記載の情報記録装置。

【請求項５】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項４に記載の情報記録装置。

【請求項６】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

2

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項４に記載の情報記録装置。

【請求項７】前記情報記録装置は、さらに、

トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、

前記暗号処理手段は、

前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、

前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする請求項４に記載の情報記録装置。

【請求項８】前記秘密情報復号処理手段は、

秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、

前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項９】前記秘密情報復号処理手段は、

秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項１０】記録媒体に記録された情報を再生する情報再生装置において、

記録媒体から読み取られるデータの復号処理を実行する暗号処理手段と、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する構成を有することを特徴とする情報再生装置。

【請求項１１】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタ

ンバーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１２】前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能とした構成を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１３】前記情報再生装置は、さらに、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成する構成であり、前記復号キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータとして構成されていることを特徴とする請求項１０に記載の情報再生装置。

【請求項１４】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項１３に記載の情報再生装置。

【請求項１５】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項１３に記載の情報再生装置。

【請求項１６】前記情報再生装置は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体からのデータの復号処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする請求項１３に記載の情報再生装置。

【請求項１７】前記秘密情報復号処理手段は、秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１８】前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１９】記録媒体に情報を記録する情報記録方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法。

【請求項２０】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする請求項１９に記載の情報記録方法。

【請求項２１】前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能としたことを特徴とする請求項１９に記載の情報記録方法。

【請求項２２】前記情報記録方法において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成するステッ

プを含み、
前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータであることを特徴とする請求項１９に記載の情報記録方法。
【請求項２３】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項２２に記載の情報記録方法。
【請求項２４】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、
前記暗号処理ステップは、
前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求項２２に記載の情報記録方法。
【請求項２５】前記情報記録方法は、さらに、
トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、
前記暗号処理ステップは、
前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、
前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求項２２に記載の情報記録方法。
【請求項２６】前記秘密情報復号処理ステップは、
秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、
該復号処理ステップは、
前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項１９に記載の情報記録方法。
【請求項２７】前記秘密情報復号処理ステップは、
秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項１９に記載の情報記録方法。
【請求項２８】記録媒体から情報を再生する情報再生方法において、
記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、
前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、
を有することを特徴とする情報再生方法。
【請求項２９】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、
前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする請求項２８に記載の情報再生方法。
【請求項３０】前記復号処理ステップは、
前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする請求項２８に記載の情報再生方法。
【請求項３１】前記情報再生方法において、
前記復号処理ステップは、
前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、
前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータであることを特徴とする請求項２８に記載の情報再生方法。
【請求項３２】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項３１に記載の情報再生方法。
【請求項３３】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、
前記復号処理ステップは、
前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする

請求項３１に記載の情報再生方法。

【請求項３４】前記情報再生方法は、さらに、

トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、

前記復号処理ステップは、

前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、

前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求項３１に記載の情報再生方法。

【請求項３５】前記秘密情報復号処理ステップは、

秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、

該復号処理ステップは、

前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項２８に記載の情報再生方法。

【請求項３６】前記秘密情報復号処理ステップは、

秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項２８に記載の情報再生方法。

【請求項３７】情報を記録可能な情報記録媒体であって、

通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、

該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体。

【請求項３８】前記秘密情報は、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする請求項３７に記載の情報記録媒体。

【請求項３９】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体。

【請求項４０】記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供するとともに、コンテンツの暗号処理用鍵の生成データとしてコンテンツの再生処理とは異なる特殊なデータ読み取り処理においてのみ読み取り可能な秘密情報を適用する構成により、コンテンツのセキュリティを高めることを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【０００２】具体的には、各記録再生器機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うとともに、コンテンツ記録、再生用のコンテンツ格納ディスクにスタンパーＩＤ等を秘密情報として格納し、特定の再生処理によって秘密情報を取得して取得秘密情報に基づいてコンテンツの暗号処理用の鍵を生成する構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム

提供媒体に関する。

【０００３】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【０００４】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【０００５】具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００６】しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【０００７】コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００８】一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００９】しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

【００１０】即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１１】そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【００１２】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができな

いようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【００１３】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【００１４】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、１つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【００１５】しかし、この方式においては、攻撃者が１つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【００１６】上記問題を解決する構成として、本出願人は、各情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばｎ分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含む有効化キーブロック（ＥＫＢ）を各情報記録再生装置に配信し、有効化キーブロック（ＥＫＢ）を受信した各情報記録再生装置のＥＫＢ復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【００１７】上述の構成は、情報記録再生装置に与えられた暗号鍵や、記録媒体へのデータの記録／再生時の暗号化／復号処理に用いるメディアキーが露呈しないことにその安全性の根拠が置かれている。従って、メディアキーの露呈が防止可能であれば問題はない。しかし、秘密とされるべきメディアキーが露呈すると、少なからずシステムに影響があるものとなっている。

【００１８】本発明は、上記の問題点を解決することを目的とするものであり、通常のデータ読み取り手法においては、データの解析が困難な構成で書き込んだ秘密情報を記録媒体へのデータの記録／再生時の暗号化／復号処理に用いる鍵生成用のデータとして用いる構成とすることにより、コンテンツの不正利用を排除可能とするとともに、記録／再生時の暗号化／復号処理に用いる鍵用の種データの漏洩の可能性を激減させたセキュリティの高い情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する構成を有することを特徴とする情報記録装置にある。

【００２０】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【００２１】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成する構成であり、読み取られた秘

密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能な構成としたことを特徴とする。

【００２２】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、さらに、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成する構成であり、前記暗号化キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータとして構成されていることを特徴とする。

【００２３】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【００２４】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【００２５】さらに、本発明の情報記録装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

【００２６】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【００２７】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【００２８】さらに、本発明の第２の側面は、記録媒体に記録された情報を再生する情報再生装置において、記録媒体から読み取られるデータの復号処理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【００２９】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【００３０】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能とした構成を有することを特徴とする。

【００３１】さらに、本発明の情報再生装置の一実施態様において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成する構成であり、前記復号キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータとして構成されていることを特徴とする。

【００３２】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特

徴とする。

【００３３】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【００３４】さらに、本発明の情報再生装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体からのデータの復号処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

【００３５】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【００３６】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【００３７】さらに、本発明の第３の側面は、記録媒体に情報を記録する情報記録方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法にある。

【００３８】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【００３９】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能としたことを特徴とする。

【００４０】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成するステップを含み、前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータであることを特徴とする。

【００４１】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【００４２】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【００４３】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

【００４４】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【００４５】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【００４６】さらに、本発明の第４の側面は、記録媒体から情報を再生する情報再生方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

【００４７】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【００４８】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行なわず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする。

【００４９】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）によって更新可能なデータであることを特徴とする。

【００５０】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【００５１】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【００５２】さらに、本発明の情報再生方法の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、前記復号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

【００５３】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を２進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記２進数系列を生成し、生成２進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【００５４】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【００５５】さらに、本発明の第５の側面は、情報を記録可能な情報記録媒体であって、通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体にある。

【００５６】さらに、本発明の情報記録媒体の一実施態様において、前記秘密情報は、複数の記録媒体において共通なスタンパーＩＤ、または個々の記録媒体に固有なディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする。

【００５７】さらに、本発明の第６の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【００５８】さらに、本発明の第７の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【００５９】

【作用】本発明の構成においては、記録媒体に、あらかじめその書き込み／読出し方法の解析の困難な秘密情報からなる信号を埋め込んでおく。この記録媒体に対してデータの記録／再生を行う際のデータの暗号化／復号処理を行うための暗号鍵には、上記の秘密情報を作用させる。秘密情報の読出し方法および読み出された秘密の値は記録再生装置内でたとえばＬＳＩ内に実装されて高度に保護され、露呈しない構成である。このような構成であるため、たとえ他の暗号鍵が露呈したとしても、記録媒体上に秘密情報として格納されたデータは安全に保護できる。また、記録媒体上の音楽等の各種コンテンツデータの暗号化／復号処理を行うための暗号鍵は、秘密情報を用いて生成されることになるため、コンテンツ自体の不正な復号等の処理が困難になり、セキュリテイレベルの高いコンテンツ保護が可能になる。

【００６０】なお、本発明の第６および第７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００６１】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００６２】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００６３】

【発明の実施の形態】［システム構成］図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ (Read Only Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、さらにトランスポート・ストリーム処理手段（ＴＳ処理手段）３００、秘密情報復号処理手段５００を有し、これらはバス１１０によって相互に接続されている。

【００６４】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００６５】暗号処理手段１５０は、例えば、１チップ

のＬＳＩ(Large Scale IntegratedCircuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００６６】ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記憶するようにしてもよい。

【００６７】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００６８】トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図６以下を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理および、記録媒体１９５からの再生処理時の出現タイミング制御処理を行なう。

【００６９】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体１９５へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（ArrivalTime Stamp：着信時刻スタンプ）を付加して記録する。

【００７０】本発明の記録再生装置１００は、上述のＡＴＳの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段１５０において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体１９５に格納する。さらに、暗号処理手段１５０は、記録媒体１９５に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【００７１】秘密情報復号処理手段５００は、記録媒体１９５に格納された特殊な再生処理により読み取り可能な秘密情報の再生、復号処理を実行する処理手段である。記録媒体１９５に格納される秘密情報は、例えばディスクの製造磁のスタンパー毎に設定されるスタンパーＩＤ、ディスク毎に異なって設定されるディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵等である。

【００７２】秘密情報復号処理手段５００は、記録媒体１９５に格納された秘密情報を読み取り復号し、復号した秘密情報を暗号処理手段１５０に転送する。暗号処理手段１５０は、秘密情報を用いて記録媒体に対するコンテンツ記録、再生時に適用する暗号処理鍵を生成する。秘密情報復号処理手段５００において復号された秘密情報は記録再生装置外部からの読み取り可能な記憶手段への格納処理を行なわず、暗号処理手段１５０内で実行されるコンテンツ暗号化キー生成においてのみ使用される構成であり、秘密情報の外部への漏洩を防止した構成となっている。

【００７３】なお、図１に示す暗号処理手段１５０、ＴＳ処理手段３００、秘密情報復号処理手段５００は、理解を容易にするため、別ブロックとして示してあるが、各機能を実行する１つまたは複数のＬＳＩとして構成してもよく、また、各機能のいずれかをソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

【００７４】本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体２０５はドラ

イブ装置としての記録媒体インタフェース（Ｉ／Ｆ）２１０から着脱が可能であり、この記録媒体２０５を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【００７５】［データ記録処理およびデータ再生処理］次に、図１あるいは図２の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図３および図４のフローチャートを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図３（Ａ）のフローチャートにしたがった記録処理が行われる。即ち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ３０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００に出力する。

【００７６】ＴＳ処理手段３００は、ステップＳ３０２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳを付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。

【００７７】暗号処理手段１５０は、ステップＳ３０３において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０に出力する。暗号化コンテンツは、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０を介して記録媒体１９５に記録（Ｓ３０４）され、記録処理を終了する。なお、暗号処理手段１５０における暗号処理については後段で説明する。

【００７８】なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

【００７９】このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ３０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

【００８０】ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

【００８１】なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

【００８２】次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図３（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ３２１において、そのアナログコンテンツを受信し、ステップＳ３２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

【００８３】このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ３２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

【００８４】以下、ステップＳＳ３２４、Ｓ３２５、Ｓ３２６において、図３（Ａ）のステップＳ３０２、Ｓ３０３における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【００８５】次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図４のフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図４（Ａ）のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ス

テップＳ４０１において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

【００８６】暗号処理手段１５０では、ステップＳ４０２において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０から供給される暗号化コンテンツが復号処理され、復号データがバス１１０を介して、ＴＳ処理手段３００に出力される。

【００８７】ＴＳ処理手段３００は、ステップＳ４０３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。入出力Ｉ／Ｆ１２０は、ＴＳ処理手段３００からのディジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるディジタルコンテンツの復号処理については後述する。

【００８８】なお、入出力Ｉ／Ｆ１２０は、ステップＳ４０４で、IEEE1394シリアルバスを介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

【００８９】記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４（Ｂ）のフローチャートに従った再生処理が行われる。

【００９０】即ち、ステップＳ４２１、Ｓ４２２、Ｓ４２３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

【００９１】ＭＰＥＧコーデック１３０では、ステップＳ４２４において、ディジタルコンテンツがＭＰＥＧデコード、すなわち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４２５）して、アナログコンテンツとする。そして、ステップＳ４２６に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【００９２】［データフォーマット］次に、図５を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

【００９３】本発明では、ＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとしている。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

【００９４】ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【００９５】なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報である。ブロック・シードは、さらにＡＴＳだけでなくコピー制御情報(ＣＣＩ：Copy Control Information)も付加した構成としてもよい。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

【００９６】なお、ここで、ブロック・シードに含まれるコピー制限情報(ＣＣＩ：Copy Control Information)は、後段で説明するが、企業５社の共同提案としての５ＣＤＴＣＰ（Digital Transmission Content Protection）システムで提唱するコピー制御情報（ＣＣＩ：Copy Control Information）であり、デバイスの能力に応じた２種類の情報、すなわち、ＥＭＩ（Encyrption Mode Indicator)、あるいは、コピー制御情報を送るための場所があらかじめ確保されているようなフォーマットにおいて適用されるコンテンツに埋め込まれたコピー制御情報（ＣＣＩ）である埋め込みＣＣＩ（Embedded CCI）のいずれかの情報を反映したものとなる。

【００９７】なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（たとえば、ｍ＝８または１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）

に制約が発生するためである。なお、もし、暗号処理が８バイト単位でなく、たとえば１バイト単位で行なえるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

【００９８】［ＴＳ処理手段における処理］ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【００９９】すなわち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームの中から１つまたは幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図７（ａ）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ（ＩＳＯ／ＩＥＣ １３８１８－１）で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【０１００】トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

【０１０１】図６に、ディジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、ディジタル放送等のディジタルデータとしてトランスポートストリームが入力される。図１または図２においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

【０１０２】トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

【０１０３】そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路６０５は、トランスポートパケットの第1バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

【０１０４】ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、ドライブ１９０（図１）、記録媒体Ｉ／Ｆ２１０（図２）を介してストレージメディアである記録媒体１９５に記録される。

【０１０５】図７は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（ａ）に示すように不規則なタイミングで現れる。

【０１０６】図７（ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（ｃ）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図７（ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【０１０７】図８は、記録媒体１９５に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

【０１０８】なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０またはディジタル入出力Ｉ／Ｆ１２０へ出力する。

【０１０９】図９は、入力ＡＶ信号を記録再生器１００

のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。従って図９は、図１または、図２おけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

【０１１０】ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥＧビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

【０１１１】端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

【０１１２】多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【０１１３】パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【０１１４】パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【０１１５】パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力されない。

【０１１６】トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着（Arrival）タイムスタンプ（time stamp）計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

【０１１７】多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

【０１１８】ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体１９５へ格納される。

【０１１９】記録媒体１９５へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体１９５に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【０１２０】ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約0.6

秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしても良い。

【０１２１】このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用する例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報（ＣＣＩ）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free）、1世代のみのコピーを許可する1世代コピー許可（One Generation Copy Allowed）、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

【０１２２】図１０に示す例３は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

【０１２３】［キー配信構成としてのツリー（木）構造について］次に、図１または図２に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図１１は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１１の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１１に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

【０１２４】各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図１１の最下段に示すＫ０００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【０１２５】図１１に示すツリー構成において、例えばデバイス０はリーフキーＫ０００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１１のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【０１２６】また、図１１のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１１に示すキー配布構成が適用されている。

【０１２７】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１１のツリー中に複数存在する。

【０１２８】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【０１２９】このツリー構造において、図１１から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの

設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【０１３０】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【０１３１】更新キーの配布処理ついて説明する。キーの更新は、例えば、図１２（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

【０１３２】図１２（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１２の例は、図１１に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１１から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【０１３３】図１２（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１２（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１２（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図１２（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【０１３４】図１１に示すツリー構造の上位段のノードキー：Ｋ０,ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１２（Ｂ）の有効化キーブロック（ＥＫＢ：Enabling Key Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【０１３５】図１２（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図１１に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図１２（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【０１３６】すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキーＫ（ｔ）masterを得ることが可能になる。

【０１３７】［ＥＫＢを使用したマスターキーの配布］図１３に、ｔ時点でのマスターキーＫ（ｔ）masterを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のマスターキーＫ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master）と図１２（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。

【０１３８】図１３に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述

したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新マスターキーＫ（ｔ）masterを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。なお、デバイス０が更新マスターキーＫ（ｔ）masterを安全に自身内に格納できる場合、リーフキーＫ００００で暗号化する必要はない。

【０１３９】また、この更新マスターキーの取得処理を図１４のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー：Ｋ（ｃ）masterを与えられ、自身のメモリに安全に（具体的にはたとえば、自身のリーフキーで暗号化して）格納しているものとする。

【０１４０】更新マスターキーＫ（ｎ）masterとＥＫＢの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップＳ１４０１において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーＫ（ｎ）masterの時点（世代）番号：ｎ（これを、プレ（pre－recording）記録世代情報（Generation#n）と呼ぶことにする）を読み出す。記録媒体には、予め、マスターキーＫ（ｎ）masterの時点（世代）番号：ｎが記憶されている。また、自身が保持している暗号化マスターキーＣを読み出し、ステップＳ１４０２において、その暗号化マスターキーの世代：ｃと、プレ記録世代情報Generation#nが表す世代：ｎとを比較して、その世代の前後を判定する。

【０１４１】ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、自身のメモリに記憶された暗号化マスターキーＣの世代：ｃよりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代：ｃが、プレ記録世代情報Generation#nが表す世代：ｎと同一か、または後の場合、ステップＳ１４０３乃至Ｓ１４０８をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキーＫ（ｃ）master（暗号化マスターキーＣ）の更新は行う必要がないので、その更新は行われない。

【０１４２】一方、ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、メモリに記憶された暗号化マスターキーＣの世代：ｃよりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎよりも前の世代である場合、ステップＳ１４０３に進み、記録再生装置は、記録媒体から、有効化キーブロック（ＥＫＢ：Enabling Key Block)を読み出す。

【０１４３】ステップＳ１４０４において、記録再生装置は、ステップＳ１４０３で読み出したＥＫＢと、自身がメモリに格納しているリーフキー（図１１のデバイス０におけるＫ００００）およびノードキー（図１１のデバイス０におけるＫ０００，Ｋ００...）を用いて、プレ記録世代情報Generation#n（図１３におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。

【０１４４】ステップＳ１４０５では、ステップＳ１４０４においてＫ（ｔ）００を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップＳ１４０６乃至Ｓ１４０８をスキップしてマスターキー更新処理を終了する。

【０１４５】Ｋ（ｔ）００を得られた場合、ステップＳ１４０６に進み、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master)、すなわち、Ｋ（ｔ）００を用いてｔ時点でのマスターキーを暗号化した値を読み出す。そしてステップＳ１４０７において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）masterを計算する。

【０１４６】ステップＳ１４０８では、自身のみが持つリーフキー（図１１のデバイス０におけるＫ００００）を用いてＫ（ｔ）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【０１４７】ところで、マスターキーは、時点（世代）０から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数ｆを保持しており、その一方向性関数ｆに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【０１４８】具体的には、例えば、記録再生装置に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、あるデータの再生に必要な（記録時に使用された）マスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＫ（ｉ－１）masterは、記録再生装置において、一方向性関数ｆが２回用いられ、ｆ（ｆ（Ｋ（ｉ＋１）master））を計算することにより生成される。

【０１４９】また、記録再生装置に記憶されているマスターキーの世代が世代ｉ＋１であり、必要なマスターキーの世代が世代ｉ－２である場合、マスターキーＫ（ｉ－２）masterは、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（Ｋ（ｉ＋１）master））)を計算することにより生成される。

【０１５０】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest 5)や、ＳＨＡ－１(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＫ（０）master，Ｋ（１）master，Ｋ（２）ma

ster・・・，K（N）masterを、あらかじめ求めておく。即ち、まず最初に、第N世代のマスターキーK（N）masterを設定し、そのマスターキーK（N）masterに、一方向性関数を１回ずつ適用しいくことで、それより前の世代のマスターキーK（N－１）master，K（N－２）master，・・・，K（１）master，K（０）masterを順次生成しておく。そして、世代の小さい（前の）マスターキーK（０）masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【０１５１】また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第０世代のマスターキーK（０）masterを設定し、そのマスターキーK（０）masterから使用していく。即ち、キー発行機関は、第１世代以降のマスターキーK（ｉ）masterが必要になったら、その１世代前のマスターキーK（ｉ－１）masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【０１５２】次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図１５のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【０１５３】まず最初に、ステップＳ１５０１において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーCの世代ｃを取得し、ステップＳ１５０２において、その暗号化マスターキーの世代ｃと、プレ記録世代情報Generation#nが表す世代ｎとを比較して、その世代の前後を判定する。

【０１５４】ステップＳ１５０２において、メモリに記憶された暗号化マスターキーCの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合、ステップＳ１５０３をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【０１５５】一方、ステップＳ１５０２において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代ｎ以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代ｎと同一か、またはそれよりも新しい場合、ステップＳ１５０３に進み、コンテンツデータの記録処理を行う。

【０１５６】［世代管理のなされたマスターキーによるコンテンツデータ暗号化および記録処理］以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。

【０１５７】図１６、図１７の処理ブロック図および図１８のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【０１５８】図１６、図１７の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理の概要について説明する。

【０１５９】記録再生装置１６００は自身のメモリ１８０（図１，２参照）に格納しているマスターキー１６０１、データ解析記録方式用キー（コグニザントキー：Cognizant Key）１６３１もしくはデータ非解析記録方式用キー（ノンコグニザントキー：Non-Cognizant Key）１６３２を読み出す。データ解析記録方式用キー（Cognizant Key）、データ非解析記録方式用キー（Non-Cognizant Key）については、後述する。

【０１６０】マスターキー１６０１は、図１４のフローにより記録再生装置のメモリに格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図１１に示す点線枠のグループに属するデバイスに共通なキーである。デバイスＩＤは記録再生装置１６００の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスＩＤは公開されていてもよい。データ解析記録方式用キー（Cognizant Key）１６３１、データ非解析記録方式用キー（Non-Cognizant Key）１６３２は、それぞれの記録モードに対応したキーであり、複数の記録再生装置に共通のキーである。これらは予め記録再生装置１６００のメモリに格納され

ている。

【０１６１】記録再生装置１６００は例えば光ディスクである記録媒体１６２０に識別情報としてのディスクＩＤ（Disc ID）１６０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）１６０３を読出し（図１６に相当）、記録されていなければ、暗号処理手段１５０においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する（図１７に相当）。ディスクＩＤ（Disc ID）１６０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【０１６２】記録再生器１６００は、次にマスターキーと、特殊な読み取り方法でのみディスクから読み取り可能な秘密情報として記録されたスタンパーＩＤ（Stamper ID）１６８０と、ディスクＩＤ１６０３を用いて、ディスク固有キー（Disc Unique Key）を生成１６０２する。

【０１６３】マスターキーと秘密情報としてのスタンパーＩＤ（Stamper ID）１６８０とディスクＩＤ１６０３とを用いディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図１９に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とスタンパーＩＤ（Stamper ID）とディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

【０１６４】上述したように、スタンパーＩＤ（Stamper ID）１６８０は、あらかじめディスクに記録されている高度な秘密情報であり、その読出しおよび読み出されたスタンパーＩＤ（Stamper ID）を利用したディスク固有キー（Disc Unique Key）の生成などの演算処理は、秘密が保たれるように暗号処理手段内部で実行される。すなわち、ディスクから読み出された秘密情報は暗号処理手段内においてセキュアに保護される。

【０１６５】このように、本発明の構成においては、特殊の読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばＬＳＩ内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【０１６６】上述したように、スタンパーＩＤ等の秘密情報は、通常のデータ書き込み手法とは異なる態様でディスクに書き込まれ、また、通常のデータ読み出しとは異なる手法でのみ読み取り可能である。この秘密情報の書き込みおよび読み出し処理構成例については後段で詳細に説明する。

【０１６７】記録再生装置１６００は、次に、記録ごとの固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１，２，参照）においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成１６０４し、ディスク１６２０に記録する。

【０１６８】さらに、この記録における記録モードがデータ解析記録方式（Cognizant Mode)かデータ非解析記録方式（Non-cognizant）かを表すフラグを設定１６３３し、ディスク１６２０に記録モード１６３５を記録する。

【０１６９】ここで、データ解析記録方式（Cognizant Mode)およびデータ非解析記録方式（Non-Cognizant Mode)について説明する。

【０１７０】コンテンツはそれぞれあらかじめコンテンツ提供者によっていかなる条件で複製が可能かを指定されている。そこで、ネットワーク接続においてもその指定された条件を正しく相手の機器に伝える必要性があり、企業５社の共同提案としての５Ｃ ＤＴＣＰ（Digital Transmission Content Protection）システムではコピー制御情報（ＣＣＩ：Copy Control Information）という方法を用いて解決している。コピー制御情報（ＣＣＩ）はデバイスの能力に応じて２種類の伝達方法が規定されている。

【０１７１】エンクリプションモード・インディケータ（ＥＭＩ：Encyrption Mode Indicator）はパケットヘッダにあるＳｙビットの上位２ビットを使ってコピー制御情報（ＣＣＩ）を送るメカニズムであり、受信デバイスが簡単にアクセスする事ができると同時に、この値がコンテンツを暗号化する鍵に作用するため安全に送ることができるようになっている。

【０１７２】ＥＭＩによりそのパケットの暗号化モードを示し、コンテンツ暗号・復号鍵の生成モードを指定する。ＥＭＩをIEEE1394パケットヘッダに置くことにより、受信機器は例えばＭＰＥＧ転送ストリーム（MPEG transport stream）の中に埋め込まれている埋め込みコピー制御情報（Embedded CCI）（後述）を取り出すことなく簡単にどのモードでコンテンツが暗号化されているかを知ることがでる。

【０１７３】図２０にＩＥＥＥ１３９４パケットフォーマットを示す。データフィールド（Data Field）中には、音楽データ、画像データ等、様々なコンテンツが格納され、コピー制御情報（ＣＣＩ）としてのエンクリプション・モード・インディケータ（ＥＭＩ：Encryption Mode Indicator）はパケットヘッダにあるＳｙビットの上位２ビットに設定される。

【０１７４】ＥＭＩの２ビット情報は、設定値に応じてコンテンツの異なる取り扱いを規定する。具体的には、値００は認証も暗号化も必要がなく、コンテンツは自由にコピーが可能なコピーフリー（Copy Free）を示し、値０１は一世代コピーの作成が可能な コピー１ジェネレーション（Copy One Generation）を、値１０は前述のCopy One Generation が一度記録された後の、再コピーが禁止されているノーモアコピー（No More Copies）を、値１１はコンテンツがリリース時点からコピー禁止であるネバーコピー（Never Copy）を表す。

【０１７５】Ｄ－ＶＨＳやハードディスクのような記録されるデータのフォーマットを認識しないようなビットストリームレコーダでも正しく著作物を取り扱えるように、記録時に埋め込みＣＣＩ（Embedded CCI）の更新（ｅｘ．Copy One Generationから No More Copies へ）を必要とせず、ＥＭＩの更新のみ行えばよい、という記録方法がデータ非解析（Non-Cognizant）記録方式である。

【０１７６】一方、こういったコピー制御情報を送るための場所があらかじめ確保されているようなフォーマット（たとえばＤＶフォーマット：DV－format）においては、ＣＣＩはコンテンツの一部として伝送することができる。このように、コンテンツの一部としてコンテンツに埋め込まれたコピー制御情報（ＣＣＩ）を埋め込みＣＣＩ（Embedded CCI）と呼ぶ。通常、コンテンツが暗号化されて転送される場合、埋め込みＣＣＩ（Embedded CCI）もコンテンツと同様に暗号化されて転送され、埋め込みＣＣＩ（Embedded CCI）の故意の変更は困難とされている。

【０１７７】ここで、前述したＥＭＩの２ビットのコピー制御情報と、埋め込みＣＣＩ（Embedded CCI）との双方を持つコンテンツの場合、コンテンツ記録を実行するある記録デバイスは、ＥＭＩおよび埋め込みＣＣＩ（Embedded CCI）の双方のコピー制御情報の更新を行なう。しかし、埋め込みＣＣＩ（Embedded CCI）の解析能力のない記録デバイスの場合、ＥＭＩは更新するが、埋め込みＣＣＩ（Embedded CCI）の更新は実行しないことになる。

【０１７８】コンテンツ記録時に、記録デバイスがコンテンツの一部として伝送された埋め込みＣＣＩ（Embedded CCI）の更新を行ってコンテンツとともに記録する記録方式をデータ解析（Cognizant）記録方式という。データ解析（Cognizant）記録方式と、データ非解析（Non-Cognizant）記録方式では、データ非解析（Non-Cognizant）記録方式の方が埋め込みＣＣＩ（Embedded CCI）の更新を行わなくてよい分、負荷が軽く実装しやすいが、５ＣＤＴＣＰのルールとして、その機器がコンテンツをＭＰＥＧデコードしてアナログ端子から映像信号を表示するためにはその機器はデータ解析記録方式（Cognizant Mode）でなければならないというルールがあり、デコード／表示機能を持つ機器はデータ解析記録方式（Cognizant Mode）を実行する機能を備えていることが必要である。

【０１７９】しかしまた、データ解析記録方式（Cognizant Mode）を実行するためには、コンテンツの一部として埋め込まれている埋め込みＣＣＩ（Embedded CCI）の位置や意味を完全に知る必要があり、たとえばある機器が市場に出た後に制定された新規のあるいは更新されたデータフォーマットについては、その新しいデータフォーマットに対して、古い機器がデータ解析記録方式（Cognizant Mode）を実行するのは非常に困難となる場合がある。

【０１８０】従って、コンテンツを記録するある機器が、特定のデータフォーマットについては、もしくは、特定の機能を実現するときには、データ解析記録方式（Cognizant Mode）を実行し、また異なるデータフォーマットのコンテンツ記録時には、データ非解析記録方式（Non-Cognizant Mode）を実行するといった、両方の記録方式を実行することが考えられる。

【０１８１】また、すべてのコンテンツに対して、データ非解析記録方式（Non-CognizantMode）の記録しか行わない機器も存在する。また、逆に埋め込みＣＣＩ（Embedded CCI）を理解できるフォーマットを持つコンテンツの処理しか実行しない機器、すなわちデータ解析記録方式（Cognizant Mode）のみ実行する機器も存在することが考えられる。

【０１８２】このように、２つのコピー制御情報、すなわちＥＭＩと埋め込みＣＣＩ（Embedded CCI）が存在し、またコンテンツ記録を実行する機器としても、データ解析記録方式（Cognizant Mode）を実行する機器と、データ非解析記録方式（Non-Cognizant Mode）の記録を実行する機器が混在する状況においては、データ解析記録方式（Cognizant Mode）で記録したコンテンツと、データ非解析記録方式（Non-Cognizant Mode）で記録したコンテンツは明確に区別されることが好ましい。

【０１８３】すなわち、データ解析記録方式（Cognizant Mode）でコンテンツを記録した場合にはＥＭＩも埋め込みＣＣＩ（Embedded CCI）の双方のコピー制御情報が更新されるが、データ非解析記録方式（Non-Cognizant Mode）でコンテンツの記録が実行された場合は、ＥＭＩのみが更新され、埋め込みＣＣＩ（Embedded CCI）の更新が行なわれない。その結果、記録媒体上のＥＭＩと埋め込みＣＣＩ（Embedded CCI）に不整合がおこり、その両者が混ざると混乱が生じるためである。従って、２つのコピー制御情報の不整合を発生させないためには、データ解析記録方式（Cognizant Mode）で記録されたコンテンツは、データ解析記録方式（Cognizant Mode）モードでの記録再生処理を実行し、データ非解析記録方式（Non-Cognizant Mode）で記録されたコンテンツはデータ非解析記録方式（Non-Cognizant Mode）モードで記録

再生処理を実行する構成とすることが必要となる。

【０１８４】このためには、このデータ解析記録方式（Cognizant Mode）と、データ非解析記録方式（Non-Cognizant Mode）とをまったく別の記録方式とすることも一案ではあるが、この場合、１つの機器において両方のモードを選択的に実行可能とするためには、１機器に両モードの実行処理構成を装備することが必要となり、これは、機器のコスト高を招くという問題がある。

【０１８５】そこで本発明の構成では、この２つの記録方式、すなわちデータ解析記録方式（Cognizant Mode）と、データ非解析記録方式（Non-Cognizant Mode）のいずれの方式を適用するかに応じて、コンテンツ暗号処理用の鍵を異なる鍵として生成して使用する構成とすることで、機器および記録方式に応じて２つの記録方式を明確に区別して、両方式が無秩序に混在して実行される事態を解消し、機器および記録方式に応じたいずれか一方の統一的な記録方式によるコンテンツ処理構成を、機器の装備および処理負荷を増大させることなく実現したものである。

【０１８６】具体的には、データ解析記録方式（Cognizant Mode）記録用の秘密情報（再生時にも必要）としての暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））をデータ解析記録方式（Cognizant Mode）による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とし、一方、データ非解析記録方式（Non-Cognizant Mode）記録用の秘密情報（再生時にも必要）としての暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））を、データ非解析記録方式（Non-Cognizant Mode）による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とした。

【０１８７】本構成により、例えば、データ解析記録方式（Cognizant Mode）で記録されたコンテンツについて、バグを原因として、あるいはデータの改竄、記録再生プログラムの不正改造等によって、データ非解析記録方式（Non-Cognizant Mode）の記録再生機能のみを有する機器において、誤ってまたは不正な記録再生の実行を防止することができる。

【０１８８】図１６、図１７に戻って、コンテンツ記録処理の説明を続ける。記録再生装置１６００は、さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号［記録時世代番号（Generation#n）］１６５０を取得して、これを記録媒体１６２０に記録時世代番号１６５１として格納する。

【０１８９】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー１６０５、記録モードフラグ１６３５、マスターキーの世代番号［記録時世代番号（Generation#n）］１６５１を格納することができる。

【０１９０】なお、記録媒体１６２０には、予め、プレ（pre－recording）世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【０１９１】次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key）、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

【０１９２】すなわち、記録モードがデータ解析記録方式（Cognizant Mode）である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）とからタイトル固有キー（Title Unique Key）を生成し、記録モードがデータ非解析記録方式（Non-Cognizant Mode）である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（TitleKey）と、データ非解析記録方式用キー（Non-Cognizant Key）とからタイトル固有キー（Title Unique Key）を生成する。

【０１９３】前述したように、データ解析記録方式（Cognizant Mode）記録用の秘密情報としての暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key）は、データ解析記録方式（Cognizant Mode）による記録または再生を行える機能を持つ機器のみが有し、一方、データ非解析記録方式（Non-Cognizant Mode）記録用の秘密情報としての暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key）は、データ非解析記録方式（Non-Cognizant Mode）による記録または再生を行える機能を持つ機器のみが有する。従って、一方の記録方式にのみ対応した機器においては、いずれか一方のモードのみを選択してコンテンツ記録が実行される。すなわち、データ解析記録方式用キー（Cognizant Key）を用いるか、あるいはデータ非解析記録方式用キー（Non-Cognizant Key）を用いるかの一方のみに限られることとなる。

【０１９４】しかし、両者のキーを格納し、両モードの記録方式を実行可能な機器においては、いずれのモードによる記録を実行するかを決定する処理が必要となる。このモード決定プロセス処理について、すなわち、コンテンツの記録をデータ解析記録方式（Cognizant Mode）によって実行するか、データ非解析記録方式（Non-Cognizant Mode）で実行するかを決定するプロセスについて図２１を用いて説明する。

【０１９５】基本的には、コンテンツ記録は、できる限りデータ解析記録方式（CognizantMode）によって実行するのが望ましい。これは、前述したように、ＥＭＩと埋

め込みＣＣＩ（Embedded CCI）との不整合を生じさせないためである。ただし、前述したように、新規なデータフォーマットの出現等によるデータ解析エラー等の発生の可能性もあり、このような場合に、データ非解析記録方式（Non-Cognizant Mode）での記録処理を実行する。

【０１９６】図２１の各ステップについて説明する。ステップＳ５００１では、記録装置は、データ・フォーマットを解析可能か否かを判定する。先に説明したように、埋め込みＣＣＩ（Embedded CCI）は、コンテンツの内部に埋め込まれており、データフォーマットの解析が不可能であれば、埋め込みＣＣＩ（Embedded CCI）の読み取りが不可能となるので、この場合は、データ非解析記録方式（Non-Cognizant Mode）での記録処理を実行する。

【０１９７】データフォーマットの解析が可能であれば、ステップＳ５００２に進み、記録装置が、データ（コンテンツ）のデコード処理、埋め込みＣＣＩ（Embedded CCI）の読み取り、更新処理が可能か否かを判定する。コンテンツおよび埋め込みＣＣＩ（Embedded CCI）は通常、符号化（エンコード）されており、埋め込みＣＣＩ（Embedded CCI）の読み取りには復号（デコード）を実行することが必要となる。例えば多チャンネル同時記録などの際に、復号回路が他に使用されているなど理由で、機器が復号処理可能でない場合は、埋め込みＣＣＩ（Embedded CCI）の読み取りができないので、データ非解析記録方式（Non-Cognizant Mode）での記録処理を実行する。

【０１９８】ステップＳ５００２のデータ（コンテンツ）のデコード処理、埋め込みＣＣＩ（Embedded CCI）の読み取り、更新処理が可能であると判定されると、ステップＳ５００３において、記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力があるか、否かが判定される。この処理は、ユーザの指定によるモード選択を可能とした機器においてのみ実行されるステップであり、通常の機器、すなわちユーザによるモード指定を許容しない機器においては実行されない。ユーザ入力によるデータ非解析記録方式（Non-Cognizant Mode）での記録処理指定があった場合は、データ非解析記録方式（Non-Cognizant Mode）での記録処理が実行される。

【０１９９】次に、ステップＳ５００４において、コンテンツパケット（ｅｘ．受信データ）中に、データ非解析モードでの記録処理の実行指定があるか否かが判定される。データ中にデータ非解析モードでの記録処理の実行指定がある場合は、データ非解析記録方式（Non-Cognizant Mode）での記録処理が実行される。指定がない場合は、データ解析記録方式（Cognizant Mode）での記録処理が実行される。

【０２００】データ解析記録方式（Cognizant Mode）での記録処理、およびデータ非解析記録方式（Non-Cognizant Mode）での記録処理の双方を選択的に実行可能な機器においては、上述したモード決定プロセス処理によって、いずれのモードでの記録を実行するかが決定される。ただし、図２１の処理フローからも理解されるように、データ解析記録方式（Cognizant Mode）での記録が可能な場合は、基本的にデータ解析記録方式（Cognizant Mode）での処理が実行されることになる。

【０２０１】前述したように、記録モードをデータ解析記録方式（Cognizant Mode）とした場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）からタイトル固有キー（Title Unique Key）を生成し、記録モードをデータ非解析記録方式（Non-Cognizant Mode）とした場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（TitleKey）と、データ非解析記録方式用キー（Non-Cognizant Key）とからタイトル固有キー（Title Unique Key）を生成する。

【０２０２】タイトル固有キー（Title Unique Key）生成の具体的な方法を図２２に示す。図２２に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、データ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode）の場合）、もしくは、データ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode）の場合）を入力して得られた結果を用いる例１の方法、あるいは、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とデータ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode）の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode）の場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

【０２０３】なお、上記の説明では、マスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデータ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-CognizantKey）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マ

スターキー（Master Key）とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（TitleUnique Key）相当の鍵を生成してもよい。

【０２０４】たとえば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス（ＳＴＢ：Set Top Box）がこの放送を記録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをＩＥＥＥ１３９４上も伝送することが、データ変換の必要がなく望ましい。

【０２０５】記録再生装置１６００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ＡＴＳとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【０２０６】ＡＴＳを付加したＴＳパケットをＸ個（例えばＸ＝３２）並べて、１ブロックのブロックデータが形成（図５の上の図参照）され、図１６、１７の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～４バイトが分離され（セレクタ１６０８）て出力される３２ビットのＡＴＳを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成１６０７される。

【０２０７】ブロック・キー（Block Key）の生成方法の例を図２３に示す。図２３では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

【０２０８】上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【０２０９】例２は、FIPS 180-1のハッシュ関数ＳＨＡ－１を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、たとえば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

【０２１０】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key）（Cognizant Mode の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）を用いてブロックキー（Block Key）を生成してもよい。

【０２１１】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１６、１７の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえばm＝８）は分離（セレクタ１６０８）されて暗号化対象とせず、ｍ＋１バイト目から最終データまでを暗号化１６０９する。なお、暗号化されないmバイト中にはブッロク・シードとしての第1～４バイトも含まれる。セレクタ１６０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化１６０９される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

【０２１２】また、前述したようにブロック・シードには、コピー制限情報（ＣＣＩ：CopyControl Information)を含ませることが可能であり、データ解析記録方式（Cognizant Mode)での記録処理を実行した場合には、コンテンツデータ内部に埋め込まれたコピー制御情報（ＣＣＩ）である埋め込みＣＣＩ（Embedded CCI）に対応するコピー制御情報が記録され、また、データ非解析記録方式（Non-CognizantMode)での記録処理を実行した場合には、図２０で説明したパケットヘッダ上のＥＭＩ（Encyrption Mode Indicator)を反映したコピー制御情報が記録される。

【０２１３】すなわち、データ解析記録方式（Cognizant Mode)による情報記録処理の場合、データ部内の埋め込みコピー制御情報（ＣＣＩ）に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行し、データ非解析記録方式（Non-Cognizant Mode)による情報記録処理の場合、パケットに含まれるコピー制御情報としてのエンクリプション・モード・インディケータ（ＥＭＩ）に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行する。

【０２１４】ここで、使用する暗号アルゴリズムのブロ

ック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、ｍを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

【０２１５】すなわち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

【０２１６】暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第1～ｍバイトデータとともにセレクタ１６１０により結合されて暗号化コンテンツ１６１２として記録媒体１６２０に格納される。

【０２１７】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ＡＴＳを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【０２１８】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【０２１９】さらに、ブロックキーは上述のようにデータ解析記録方式（Cognizant Mode)の記録の場合は、データ解析記録方式用キー（Cognizant Key)に基づいて生成され、データ非解析記録方式（Non-Cognizant Mode）記録の場合は、データ非解析記録方式用キー（Non-Cognizant Key)に基づいて生成される。これらの暗号化データは、記録時と同一のモードに対応する鍵（データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key））を持つ機器でのみ再生可能となる。

【０２２０】すなわち、データ解析記録方式用キー（Cognizant Key)は、記録時にストリーム中に埋め込まれた Embedded CCI を認識して必要に応じて更新する能力を持つ機器およびそのデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ解析記録方式（Cognizant Mode)で記録されたコンテンツの再生は行えない。

【０２２１】同様に、データ非解析記録方式用キー（Non-Cognizant Key)は、記録時にストリーム中の埋め込みＣＣＩ（Embedded CCI）を認識しないデータ非解析記録方式(Non-Cognizant)の記録モードの機能を持つ機器と、そのモードで記録されたデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ非解析記録方式（Non-Cognizant Mode)で記録されたコンテンツの再生は行えないようになっている。なお、再生処理の詳細については後述する。

【０２２２】次に図１８に示すフローチャートに従って、データ記録処理にともなって実行されるＴＳ処理手段３００におけるＡＴＳ付加処理および暗号処理手段１５０における暗号処理の処理全体の流れをまとめて説明する。図１８のＳ１８０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキーおよびデータ解析記録方式用キー（Cognizant Key）（データ解析記録方式（CognizantMode)の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）を読み出す。また、ディスクからスタンパーＩＤ(Stamper ID)を読み出す。

【０２２３】Ｓ１８０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ１８０３でこのディスクＩＤを読出し、記録されていなければＳ１８０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ１８０５では、マスタキーと スタンパーＩＤ(Stamper ID)とディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【０２２４】次にＳ１８０６に進み、その一回の記録ごとの固有の鍵としてのタイトルキー（Title Key）を生成し、記録モード（Recording Mode）とマスターキーの世代番号とともにディスクに記録する。記録モード（Recording Mode）は、実行する情報記録モードが、データ解析記録方式（Cognizant Mode)であるか、データ非解析記録方式（Non-Cognizant Mode)であるかを示す。

【０２２５】次にＳ１８０７で、上記のディスク固有キーとタイトルキーと、データ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode)の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）から、タイトル固有キーを生成する。

【０２２６】タイトル固有キーの生成の詳細フローを図２４に示す。暗号処理手段１５０は、ステップＳ２００１において、記録モードにより分岐する。この分岐は、記録再生器のプログラムや、記録再生器を使用するユーザによって入力された指示データに基づいて判定される。

【０２２７】Ｓ２００１で記録モードがデータ解析記録方式（Cognizant Mode)、すなわち、Cognizant 記録の場合は、ステップＳ２００２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)とから、タイトル固有キー（Title Unique Key）を生成する。

【０２２８】Ｓ２００１で記録モードがデータ非解析記

録方式 (Non-Cognizant Mode)、すなわち、Non-Cognizant 記録の場合は、ステップＳ２００３に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key)とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【０２２９】Ｓ１８０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１８０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１８１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１８１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

【０２３０】次に、暗号処理手段１５０は、Ｓ１８１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１８０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【０２３１】Ｓ１８１３では、ブロックキーを用いてＳ１８１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ (Data Encryption Standard) が適用される。

【０２３２】Ｓ１８１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ１８１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ１８０８に戻って残りのデータの処理を実行する。

【０２３３】上述の処理にしたがって、コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) あるいは、データ非解析記録方式 (Non-Cognizant Mode)のいずれかによって実行される。コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵が、データ解析記録方式用キー (Cognizant Key)に基づいて生成され、また、コンテンツの記録処理がデータ非解析記録方式 (Non-Cognizant Mode)で実行される場合は、コンテンツの暗号化に適用される鍵がデータ非解析記録方式用キー (Non-Cognizant Key)に基づいて生成されることになる。従って、それぞれの方式においてディスクに記録されたコンテンツは、記録時に使用したデータ解析記録方式用キー (Cognizant Key)、あるいはデータ非解析記録方式用キー (Non-Cognizant Key)のいずれか、同一のキーを適用して復号用の鍵を生成することが必須となり、各方式が混在した記録、再生処理が防止される。

【０２３４】［秘密情報の書き込みおよび再生］次に、図１６、図１７等に示したスタンパーＩＤ等の秘密情報を、通常のデータ書き込み手法とは異なる態様でディスクに書き込み、また、通常のデータ読み出しとは異なる手法を適用した場合にのみ読み取り可能な態様とした秘密情報の書き込みおよび読み出し処理構成例について説明する。

【０２３５】（信号の擾乱による秘密情報生成）まず、スタンパーＩＤ等の各種情報信号をM系列信号により擾乱して記録する構成について説明する。

【０２３６】図２５に秘密情報の書き込み処理のための書き込み信号生成変調回路構成を示す。図２５に示す変調回路は、データ書き込み対象であるディスク原盤が、所定の角度だけ回転する毎に信号レベルが立ち上がるＦＧ信号を基準にしてスタンパＩＤ等の秘密情報の変調を行ない書き込みを実行する。

【０２３７】ＰＬＬ回路１０４１は、ＦＧ信号を基準にディスク原盤の回転に同期したチャンネルクロックＣＫを生成して変調回路の各部に供給する。

【０２３８】タイミングジェネレータ１０４２は、チャンネルクロックＣＫをカウントすることにより、所定の時間間隔でM系列発生回路１０４５Ａ～１０４５Ｄを初期化する初期化パルスＳＹを発生する。また、タイミングジェネレータ１０４２は、初期化パルスＳＹに同期した同期パターン選択信号ＳＴを生成して出力する。

【０２３９】図２５に示す変調回路においては、チャンネルクロックＣＫに対して格段に遅いビットレートでスタンパーＩＤ等の秘密情報が入力される。同期パターン発生回路１０４３は、初期化パルスＳＹの立上がりを基準にして所定の同期パターンＤＹを生成して出力する。

【０２４０】M系列発生回路１０４５ａ～１０４５Ｄは、初期化パルスＳＹにより初期化され、チャネルクロックＣＫ単位で変化するM系列Ｍ１～Ｍ４を出力する。ここでM系列Ｍ１～Ｍ４は、ランダムに論理値が変化し、かつ論理１と論理０との発生確率が等確立であるデータ列であり、相互に無相関である。

【０２４１】演算回路（Ｘ）１０４６Ａ～１０４６Ｄは、エクスクルーシブオア回路により構成され、それぞれM系列信号Ｍ１～Ｍ４と、スタンパＩＤ、ディスクＩＤ等の秘密情報の各ビットｂ０～ｂ３とエクスクルーシブオア演算を実行して演算結果を出力する。これにより、スタンパーＩＤ等の秘密情報は、M系列信号Ｍ１～Ｍ４により擾乱される。

【０２４２】乱数発生回路１０４７は、２ビットの乱数（０，１，２，３のいずれかの値）Ｒをチャネルクロックｃｋ単位で発生し、データセレクタ１０４８に出力す

る。データセレクタ１０４８は、乱数Ｒの値に応じて演算回路１０４６Ａ～１０４６Ｄの演算結果を選択出力する。例えば乱数Ｒ＝０のとき演算回路１０４６Ａの出力選択、乱数Ｒ＝１とき演算回路１０４６Ｂの出力選択、乱数Ｒ＝２のとき演算回路１０４６Ｃの出力選択、乱数Ｒ＝３のとき演算回路１０４６Ｄの出力選択とする。

【０２４３】この構成により、変調回路は、対応するＭ系列Ｍ１～Ｍ４を基準にした復号により他の演算結果による影響を受けずに１０４６Ａ～１０４６Ｄの演算結果を１系統としてさらに擾乱する構成を可能としている。

【０２４４】データセレクタ１０４９は、同期パターン信号ＳＴを基準にして同期パターン発生回路１０４３から出力される同期パターンＤＹ、データセレクタ１０４８の出力を選択出力する。これにより、初期化パルスＳＹが立ち上がった後、所定のクロック周期、例えば5クロック周期の間同期パターン［ｅｘ．１１０１１］の後、データセレクタ１０４８の出力を行なう。

【０２４５】ディスク原盤には、所定の秘密情報書き込み領域に図２５に示す変調回路において生成された出力が書き込まれる。変調回路に入力されるスタンパーＩＤ等の秘密情報が同一でも、乱数に応じて書き込みデータ態様が異なることになる。従って通常の読み出し処理においては解析困難なデータの書き込みが可能となる。

【０２４６】次に、上述の手法で書き込まれた秘密情報の再生処理について、図２６を用いて説明する。図２６は、ディスクから読み取られたディジタル再生信号ＤＸからスタンパーＩＤ等の秘密情報を復号する復号処理手段構成を示す図である。ＰＬＬ回路１０８１は、ディスクから読み取られたディジタル再生信号ＤＸを基準にして記録時に生成したチャネルクロックＣＫを再生して各部に出力する。

【０２４７】同期検出回路１０８２は、チャネルクロックＣＫを基準にしたディジタル再生信号ＤＸの識別により同期パターンを検出し、検出結果により記録時の初期化パルスＳＹを再生する。Ｍ系列発生回路１０８３Ａ～１０８３Ｄは、この初期化パルスＳＹ、チャネルクロックＣＫを基準にして、それぞれ記録時に生成したＭ系列Ｍ１～Ｍ４を出力する。

【０２４８】乗算回路（Ｘ）１０８４Ａ～１０８４Ｄは、それぞれＭ系列信号Ｍ１～Ｍ４とディジタル再生信号ＤＸを乗算して乗算結果を出力する。なお、ここで乗算回路（Ｘ）１０８４Ａ～１０８４Ｄは、Ｍ系列信号Ｍ１～Ｍ４の論理値に応じてディジタル再生信号ＤＸの極性を反転することにより、この乗算処理を実行する。ディジタル再生信号ＤＸは、対応するＭ系列Ｍ１～Ｍ４を基準にした復号によってのみ正しく再生される。

【０２４９】積分回路１０８５Ａ～１０８５Ｄは、乗算回路１０８４Ａ～１０８４Ｄにより出力される乗算結果をそれぞれ初期化パルスＳＹを基準にして積分することにより、スタンパーＩＤ等の秘密情報の対応するビット列ｂ１～ｂ３の論理値に応じた値の積分結果を出力する。判定回路１０８６Ａ～１０８６Ｄは、それぞれ積分回路１０８５Ａ～１０８５Ｄより出力される積分結果を初期化パルスＳＹを基準にして２値識別することにより、スタンパーＩＤ等の秘密情報の各ビットｂ０～ｂ３を復号して出力する。

【０２５０】上述したように、スタンパーＩＤ等の秘密情報は、４ビットパラレルビット列ｂ０～ｂ３として変調回路（図２５）に入力され、４系統のＭ系列Ｍ１～Ｍ４、また乱数Ｒによる擾乱がなされて記録されるので、通常の読み出し処理での読み取りが困難となる。また、再生時には同期パターンＤＹを基準にしてＭ系列Ｍ１～Ｍ４を生成可能となり、生成したＭ系列により、読み取り信号の復号により、スタンパーＩＤ等の秘密情報の出力が可能となる。

【０２５１】上述の記録方式により書き込まれたスタンパーＩＤを読み取り、スタンパーＩＤ等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図２６の構成を持つ秘密情報復号処理手段構成を持つ。

【０２５２】（ディスク内周に秘密情報を記録）次に、秘密情報の書き込み、再生処理の異なる例として、音楽データ等の書き込み領域とは異なるディスク領域にスタンパＩＤ等の秘密情報を書き込み、これをフォーカスサーボにより安定的に読み取ることを可能とした構成について説明する。

【０２５３】図２７は、スタンパＩＤ等の秘密情報を記録したディスクを示す斜視図である。スタンパーＩＤ等の秘密情報は、ディスクの１周に４回繰り返し記録され、部分的に損傷が発生した場合でも秘密情報の再生が可能となるように構成される。秘密情報は、ヘッダー、スタンパーＩＤ等の情報領域、さらに誤り訂正符号が割り当てられた構成を持つ。これらの情報を示すビットパターンの各ビットは、ユーザデータとして記録されるデータ領域の各ビットに比較して格段に長い、例えば５０μｍ単位の微少領域を単位として形成される。また、スタンパーＩＤの情報領域、誤り訂正符号領域には、３つの微少領域の中心領域のみ、記録面の光学特性を変化させたパターンが形成された同期パターンが形成され、この同期パターンにより、再生時のタイミング制御が可能となる。

【０２５４】また、スタンパーＩＤ等の情報領域、誤り訂正符号領域データは、２ビット毎にデータを区切り、２ビットデータ（ｂ１，ｂ０）が、論理００の場合、図２７（Ｄ１）に示すように、先頭の微少領域のみの記録面の光学特性を変化を発生させ、論理［１０００］に変換して記録する。以下、（Ｄ２）２ビットデータ（ｂ１，ｂ０）が、論理０１の場合、［０１００］、（Ｄ３）２ビットデータ（ｂ１，ｂ０）が、論理１０の場合、［００１０］、（Ｄ４）２ビットデータ（ｂ１，ｂ０）が、論理１１の場合、［０００１］とする。これに

より、ディスク上には、光学特性の変化した領域の存在比率が０．３以下となり、ディスク内周領域においても十分な反射光量によるフォーカスサーボを可能としてデータ読み取りを可能となる。

【０２５５】図２８は、ディスク内周領域に記録したスタンパーＩＤ等の秘密情報の読み取りに用いられる復号処理手段構成を示した図である。ＰＬＬ回路１１６０は、ディジタル再生信号ＤＸよりチャネルクロックＣＫを再生出力する。

【０２５６】同期検出回路１１６１は、チャネルクロックＣＫを基準にしてディジタル再生信号ＤＸの信号レベルを判定することにより、同期パターンを検出して初期化パルスＳＹを出力する。

【０２５７】タイミングジェネレータ１１６２は、初期化パルスＳＹを基準にして、同期パターンに続く図２７に示す第１～４の微少領域について、それぞれ各微少領域のほぼ中央で立ち上がるサンプリングパルスＴ１～Ｔ４を出力する。

【０２５８】フリップフロップ（ＦＦ）１１６３Ａ～１１６３Ｄは、、それぞれサンプリングパルスＴ１～Ｔ４を基準にしてディジタル再生信号をラッチする。これにより、スタンパＩＤ、ディスクＩＤ等の情報領域、誤り訂正符号領域データの各２ビットに割り当てた４つの微少領域より得られる再生信号の信号レベルを、それぞれフリップフロップ１１６３Ａ～１１６３Ｄにラッチして保持する。

【０２５９】最大値検出回路１１６４は、これら４つのラッチＤ１～Ｄ４の大小判定により、スタンパーＩＤ、ディスクＩＤ等の情報領域、誤り訂正符号領域の２ビットデータ（ｂ１，ｂ０）を復号して出力し、パラレルシリアル変換回路（ＰＳ）１１６５は、順次、最大値検出回路１１６４より出力される２ビットデータ（ｂ１，ｂ０）をシリアルデータに変換して出力する。

【０２６０】上述の記録方式により書き込まれたスタンパーＩＤを読み取り、スタンパーＩＤ等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図２８の構成を秘密情報復号処理手段構成を持つ。

【０２６１】このように、コンテンツとは異なる特殊な秘密情報書き込み手法と読み取り手法の構成を採用して、スタンパーＩＤ等の秘密情報をディスクに格納し、これをコンテンツの暗号化、復号処理に適用する鍵の元データとして使用する構成としたので、たとえ他の処理キーが漏洩したとしても、ディスクに格納されたスタンパーＩＤ等の秘密情報は読み取りが困難であり、漏洩の可能性を激減させることが可能となり、よりセキュリティを高めたコンテンツ保護が可能となる。

【０２６２】なお、本明細書においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーＩＤとして設定した例を説明するが、スタンパーＩＤに限らず、ディスク毎に異なって設定されるディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【０２６３】なお、上述した記録再生装置は、図１６，図１７に示すように、データ解析記録方式（Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成であるが、いずれか一方のみの方式を実行する記録再生機器においては、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録方式用キー（Non-Cognizant Key）のみを格納しており、格納キーに基づいてコンテンツの暗号化、復号処理用のブロックキーを生成する。これら単独のキーを格納した記録再生装置におけるコンテンツの暗号処理キーの生成処理過程を示すブロック図を図２９、図３０に示す。

【０２６４】図２９は、データ解析記録方式用キー（Cognizant Key）のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ解析記録方式用キー（Cognizant Key）他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【０２６５】図３０は、データ非解析記録方式用キー（Non-Cognizant Key）のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ非解析記録方式用キー（Non-Cognizant Key）他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【０２６６】これらの単独キー格納装置においては、いずれか一方の方式においてのみデータの記録、再生が実行可能となる。

【０２６７】［世代管理のなされたマスターキーによるコンテンツデータ復号および再生処理］次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図３１の処理ブロック図と、図３２～図３４のフローチャートを用いて説明する。

【０２６８】図３１の処理ブロック図を参照しながら、図３２に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図３２のＳ２４０１において、記録再生装置２３００（図３１参照）はディスク２３２０からディスクＩＤ２３０２とプレ（pre－recording）記録世代番号とスタンパーＩＤ(S

tamper ID)２３８０を読み出し、また自身のメモリからマスターキー２３０１、データ解析記録方式用キー (Cognizant Key)２３３１および／あるいはデータ非解析記録方式用キー (Non-Cognizant Key)２３３２を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

【０２６９】プレ (pre－recording) 記録世代番号２３６０は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ (pre－recording) 世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号２３５０を比較して再生処理の可否を制御する。マスターキー２３０１は、図１４のフローにより記録再生装置のメモリに格納され世代管理のなされた秘密キーである。データ解析記録方式用キー (Cognizant Key)およびデータ非解析記録方式用キー (Non-Cognizant Key)は、それぞれデータ解析 (Cognizant) 記録モードおよびデータ非解析 (Non-Cognizant) 記録モードに対応したシステム共通の秘密キーである。

【０２７０】記録再生装置２３００は、次に、Ｓ２４０２で、ディスクから読み出すべきデータのタイトルキー、さらに、データの記録モード、データを記録したときに使用したマスターキーの世代番号 (Generation #) すなわち記録時世代番号２３５０を読み出す。次に、Ｓ２４０３で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図３３に示す。

【０２７１】図３３のステップＳ２５０１において、記録再生装置は、Ｓ２４０１で読み出したプレ世代番号と、Ｓ２４０２で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【０２７２】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【０２７３】一方、ステップＳ２５０１において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代ｎと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップＳ２５０２に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーＣの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

【０２７４】ステップＳ２５０２において、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。

【０２７５】一方、ステップＳ２５０２において、メモリに記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップＳ２５０３に進み、記録時のモードに対応する鍵、すなわちデータ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)を、再生機器自身が所有しているかどうかを判断する。

【０２７６】ステップＳ２５０３において、記録時のモードに対応する鍵であるデータ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)を、再生機器自身が所有している場合、再生可能と判定する。記録時のモードに対応する鍵 (データ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)) を、再生機器自身が所有していない場合、再生不可能と判定する。

【０２７７】再生可能と判定された場合は、ステップＳ２４０４に進む。Ｓ２４０４では、ディスクＩＤ (Disc ID) とマスターキー (Master Key) とスタンパーＩＤ (Stamper ID)を用いてディスク固有キー (Disc Unique Key) を生成２３０２する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ (Disc ID) とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクＩＤ (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、図３２のステップＳ２４０２で記録媒

体から読み出した、そのデータの記録時世代番号が表す世代（時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

【０２７８】次に、Ｓ２４０５で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図３４に示す。暗号処理手段１５０は、ステップＳ２６０１において、記録モードの判定を実行する。この判定は、ディスクから読み出した記録モード（Recording Mode）に基づいて実行される。

【０２７９】Ｓ２６０１において、記録モードがデータ解析記録方式（Cognizant Mode)であると判定された場合は、ステップＳ２６０２に進み、ディスク固有キー（DiscUnique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)とから、タイトル固有キー（Title Unique Key）を生成する。

【０２８０】Ｓ２６０１において、記録モードがデータ非解析記録方式（Non-Cognizant Mode)であると判定された場合は、ステップＳ２６０３に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key）とから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【０２８１】なお、上記の説明では、マスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデータ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０２８２】次にＳ２４０６でディスクから暗号化されて格納されている暗号化コンテンツ２３１２から順次ブロックデータ（Block Data）を読み出し、Ｓ２４０７で、ブロックデータの先頭の４バイトのブロック・シード（Block Seed）をセレクタ２３１０において分離して、ブロックシード（Block Seed）と、Ｓ２４０５で生成したタイトル固有キーを用いてブロックキーを生成する。

【０２８３】ブロック・キー（Block Key）の生成方法は、先に説明した図２３の構成を適用することができる。すなわち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

【０２８４】なお、上記説明ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)を用いてブロックキー（Block Key）を生成してもよい。

【０２８５】ブロックキーが生成されると、次にＳ２４０８で、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号２３０９し、セレクタ２３０８を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を再生したりすることが可能となる。

【０２８６】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ２４０９で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ２４０６に戻り残りのデータを読み出す。

【０２８７】なお、上述した記録再生装置は、図３１に示すように、データ解析記録方式（Cognizant Mode)記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode)記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成例であるが、先に図２９、図３０に示して説明したように、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録

方式用キー（Non-Cognizant Key）のみを格納した機器においては、いずれか一方のみの格納キーに対応する方式のみを実行し、格納キーに基づいてコンテンツの復号処理用のブロックキーを生成する。

【０２８８】［記録媒体にのみ有効なメディアキーを使用した処理構成］ところで、上記の実施例においては、有効化キーブロック（ＥＫＢ：EnablingKey Block）を用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

【０２８９】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【０２９０】これに対し、記録媒体のＥＫＢ（Enabling Key Block）を用いて伝送する鍵を、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることにより、キーの露呈の影響を抑えることが可能となる。以下に、第２の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第１の実施例との変更部分のみを説明する。

【０２９１】図３５には、図１３と同様の例として、デバイス０が記録媒体に格納されている ｔ 時点のＥＫＢと自分があらかじめ格納しているリーフキーＫ００００とノードキーＫ０００，Ｋ００を用いて更新ノードキーＫ（ｔ）００を生成し、それを用いて更新メディアキー：Ｋ（ｔ）mediaを得る様子を示している。ここで得たＫ（ｔ）mediaは、その記録媒体のデータの記録、再生時に使用される。

【０２９２】なお、図３５におけるプレ記録世代番号（Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【０２９３】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図３６に示すフローチャートによってその記録媒体用のメディアキー：Ｋ（ｔ）mediaを計算し、後にその記録媒体へのアクセスに使用する。

【０２９４】図３６のステップＳ２８０１のＥＫＢの読みこみとＳ２８０２のＥＫＢの処理は、それぞれ図１４のステップＳ１４０３およびＳ１４０４と同様の処理である。

【０２９５】ステップＳ２８０３において記録再生装置はメディアキーＫ（ｔ）mediaをノードキー Ｋ（ｔ）００で暗号化した暗号文Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media)を記録媒体から読みこみ、ステップＳ２８０４でこれを復号してメディアキーを得る。もしこの記録再生装置が図１１に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【０２９６】次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第１の実施例において図１５に示した、プレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図３７に示す処理フローのようになる。図３７の処理フローは、メディアキーの取得をＳ２９０１で判定し、取得された場合にのみ、ステップＳ２９０２においてコンテンツの記録処理を実行するものである。

【０２９７】［記録媒体にのみ有効なメディアキーを使用したデータの記録処理］コンテンツデータの記録処理の様子を、図３８、３９のブロック図および図４０のフローチャートを用いて説明する。

【０２９８】本実施例では、第１の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

【０２９９】図３８および図３９は、それぞれ第１の実施例における図１６および図１７に対応する図であり、マスターキー（Master Key）の代わりにメディアキー（Media Key）が使われている点が異なっており、また、マスターキーの世代を示す記録時世代番号（Generation #）を用いていない点が異なっている。図３８および図３９の差異は、図１６、図１７の差異と同様ディスクＩＤの書き込みを実行するかしないかの差異である。

【０３００】図４０はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図１８（実施例１）のフローチャートに対応する。以下、図４０の処理フローについて実施例１と異なる点を中心として説明する。

【０３０１】図４０のＳ３２０１において、記録再生装置３０００は自身のメモリに格納している データ解析記録方式用キー（Cognizant Key)および／もしくはデータ非解析記録方式用キー（Non-Cognizant Key)と、図３６のＳ２８０４で計算し、一時的に保存しているメディアキーＫ（ｔ）mediaを読み出す。また、ディスクからスタンパーＩＤ(Stamper ID)を読み出す。

【０３０２】Ｓ３２０２において、記録再生装置は記録媒体（光ディスク）３０２０に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、Ｓ３２０３でこのディスクＩＤ（Disc ID）を読出し（図３８に相当）、記録され

ていなければ、Ｓ３２０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤ（Disc ID）を生成し、ディスクに記録する（図３９に相当）。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にＳ３２０５に進む。

【０３０３】Ｓ３２０５では、Ｓ３２０１で読み出したメディアキーと スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、第１の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【０３０４】次にＳ３２０６に進み、その一回の記録ごとに固有の鍵：タイトルキー（Title Key）をランダムに、あるいはあからじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル（データ）を記録したときの記録モード（Recording Mode）をディスクに記録する。

【０３０５】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、RecordingMode を格納することができる。

【０３０６】ステップＳ３２０７乃至Ｓ３２１５は図１８のＳ１８０７乃至Ｓ１８１５と同様であるため説明を省略する。

【０３０７】なお、上記の説明では、メディアキー（Media Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）と データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（TitleKey）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０３０８】以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【０３０９】［記録媒体にのみ有効なメディアキーを使用したデータの再生処理］次に、上記のようにして記録されたデータを再生する処理の様子を図４１のブロック図と図４２のフローチャートを用いて説明する。

【０３１０】図４１は、第１の実施例における図３１に対応する図であり、マスターキー（Master Key）の変わりにメディアキー（Media Key）が使われ、そのため記録時世代番号（Generation #）が省略されている点が異なっている。

【０３１１】図４２のＳ３４０１において、記録再生装置３４００は記録媒体であるディスク３４２０からスタンパーＩＤ(Stamper ID)およびディスクＩＤ（Disc ID）を、また自身のメモリからデータ解析記録方式用キー（Cognizant Key)および／あるいはデータ非解析記録方式用キー（Non-Cognizant Key)と、図３６のＳ２８０４で計算し一時的に保存しているメディアキーを読み出す。

【０３１２】なお、この記録媒体の挿入時に、図３６の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【０３１３】次にＳ３４０２で、ディスクから読み出すべきデータのタイトルキー（TitleKey）とこのデータを記録した際の記録モード Recording Mode を読み出す。

【０３１４】次にＳ３４０３で、このデータが再生可能であるか否かを判断する。Ｓ３４０３の処理の詳細を図４３に示す。

【０３１５】ステップＳ３５０１ではメディアキー（Media Key）を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップＳ３５０２に進む。ステップＳ３５０２の処理は図３３のＳ２５０３と同じであり、そのデータの記録時に使われた記録モードに対応する鍵（データ解析記録方式（Cognizant Mode)の場合、データ解析記録方式用キー（Cognizant Key),データ非解析記録方式（Non-Cognizant Mode)の場合、データ非解析記録方式用キー（Non-Cognizant Key)）を再生機器が持っている場合には「再生可能」と判断してステップＳ３４０４に進み、それ以外の場合には、「再生不可能」と判断して、ステップＳ３４０４乃至Ｓ３４０９をスキップして、再生処理を行わずに処理を終了する。

【０３１６】ステップＳ３４０４乃至Ｓ３４０９の処理は、図３２のＳ２４０４乃至Ｓ２４０９と同様であるため、説明を省略する。

【０３１７】なお、上記の説明では、メディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とスタンパ

ーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー(Cognizant Key)もしくはデータ非解析記録方式用キー(Non-Cognizant Key)から直接タイトル固有キー（Title UniqueKey）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０３１８】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

【０３１９】［記録処理におけるコピー制御］さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【０３２０】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【０３２１】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図１または図２の記録再生装置の処理について、図４４および図４５のフローチャートを参照して説明する。

【０３２２】まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図４４（Ａ）のフローチャートにしたがった記録処理が行われる。図４４（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ４００１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ４００２に進む。

【０３２３】ステップＳ４００２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

【０３２４】また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【０３２５】記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【０３２６】ステップＳ４００２において、コンテンツがコピー可能でないと判定された場合、ステップＳ４００３～Ｓ４００５をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０３２７】また、ステップＳ４００２において、コンテンツがコピー可能であると判定された場合、ステップＳ４００３に進み、以下、ステップＳ４００３～Ｓ４００５において、図３（Ａ）のステップＳ３０２、Ｓ３０３、Ｓ３０４における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【０３２８】なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

【０３２９】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【０３３０】本発明の記録再生装置では、このＥＭＩやembedded CCIなどのコピー制御情報を、ＴＳパケットに付加する形で記録する。即ち、図１０の例２や例３のように、ＡＴＳを２４ビットないし３０ビット分と、コピー制御情報を加えた３２ビットを図５に示すように各ＴＳパケットに付加する。

【０３３１】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図４４（Ｂ）のフローチャートにしたがった記録処理が行われる。図４４

（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ４０１１において、そのアナログコンテンツを受信し、ステップＳ４０１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【０３３２】ここで、ステップＳ４０１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【０３３３】また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【０３３４】従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【０３３５】さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【０３３６】ステップＳ４０１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ４０１３乃至Ｓ４０１７をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０３３７】また、ステップＳ４０１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ４０１３に進み、以下、ステップＳ４０１３乃至Ｓ４０１７において、図３（Ｂ）のステップＳ３２２乃至Ｓ３２６における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、ＭＰＥＧ符号化、ＴＳ処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【０３３８】なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。即ち、図１０で示したＣＣＩもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０３３９】［再生処理におけるコピー制御］次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図４５（Ａ）のフローチャートにしたがった再生処理が行われる。図４５（Ａ）の処理について説明する。まず最初に、ステップＳ４１０１、Ｓ４１０２、Ｓ４１０３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、ＴＳ処理がなされる。各処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

【０３４０】入出力Ｉ／Ｆ１２０は、ステップＳ４１０４において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０３４１】また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格にしたがって、ＥＭＩ等のコピー制御情報が記録された場合には、そのＥＭＩ（記録されたＥＭＩ(Recorded EMI)）等のコピー制御情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩ等のコピー制御情報が、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【０３４２】なお、一般的には、記録されたＥＭＩ等のコピー制御情報が、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０３４３】ステップＳ４１０４において、コンテンツが、後でコピー可能なものであると判定された場合、ス

テップＳ４１０５に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

【０３４４】また、ステップＳ４１０４において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ４１０６に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等にしたがって、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０３４５】即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０３４６】このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

【０３４７】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４５（Ｂ）のフローチャートにしたがった再生処理が行われる。図４５（Ｂ）の処理について説明する。ステップＳ４１１１乃至Ｓ４１１５において、図４（Ｂ）のステップＳ４２１乃至Ｓ４２５における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＴＳ処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

【０３４８】入出力Ｉ／Ｆ１４０は、ステップＳ４１１６において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにＥＭＩ等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０３４９】また、コンテンツの記録時に、たとえばＤＴＣＰの規格にしたがって、ＥＭＩ等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【０３５０】また、ＥＭＩ等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【０３５１】さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【０３５２】ステップＳ４１１６において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ４１１７に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【０３５３】また、ステップＳ４１１６において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ４１１８に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０３５４】即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０３５５】このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、CGMS－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【０３５６】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【０３５７】［データ処理手段の構成］なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップ

のマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にＴＳ処理手段３００も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図４６は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０３５８】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク４２０５やＲＯＭ４２０３に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体４２１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体４２１０は、いわゆるパッケージソフトウエアとして提供することができる。

【０３５９】なお、プログラムは、上述したようなリムーバブル記録媒体４２１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部４２０８で受信し、内蔵するハードディスク４２０５にインストールすることができる。

【０３６０】コンピュータは、ＣＰＵ(Central Processing Unit)４２０２を内蔵している。ＣＰＵ４２０２には、バス４２０１を介して、入出力インタフェース４２１１が接続されており、ＣＰＵ４２０２は、入出力インタフェース４２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部４２０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)４２０３に格納されているプログラムを実行する。

【０３６１】あるいは、ＣＰＵ４２０２は、ハードディスク４２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部４２０８で受信されてハードディスク４２０５にインストールされたプログラム、またはドライブ４２０９に装着されたリムーバブル記録媒体４２１０から読み出されてハードディスク４２０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)４２０４にロードして実行する。

【０３６２】これにより、ＣＰＵ４２０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ４２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース４２１１を介して、ＬＣＤ(Liquid CryStal Display)やスピーカ等で構成される出力部４２０６から出力、あるいは、通信部４２０８から送信、さらには、ハードディスク４２０５に記録させる。

【０３６３】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０３６４】また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０３６５】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１および図２に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

【０３６６】［記録媒体の製造装置および方法］次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置および方法について説明する。

【０３６７】図４７には、記録媒体を製造すると共に、記録媒体に対してディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

【０３６８】この図４７に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録し、前述の秘密情報を記録する。さらに、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）も併せて記録する。

【０３６９】ディスク製造装置４３００は、ディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーをあらかじめ格納しているメモリ４３０２もしくはその他の記憶手段と、記録媒体４３５０に対する読み書きを行う記録媒体Ｉ／Ｆ４３０３と、他の装置とのＩ／Ｆとなる入出力Ｉ／Ｆ４３０４と、それらを制御する制御部４３０１、これらを接続するバス４３０５を備えている。

【０３７０】なお、図４７の構成では、メモリ４３０２および記録媒体Ｉ／Ｆ４３０４は、当該製造装置に内蔵されている例を挙げているが、メモリ４３０２および記録媒体Ｉ／Ｆ４３０３は外付けのものであってもよい。

【０３７１】上記のディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling KeyBlock）および、暗号化されたマスターキーまたは暗号化されたメディアキー、スタンパーＩＤ等の秘密情報、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、たとえば図示しない識別子管理部門、鍵発行センター等により発行されるものであり、上記内蔵あるいは外付けのメモリにあらかじめ格納されている。

【０３７２】上記メモリ４３０２に格納されているディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）、スタンパーＩＤ等の秘密情報および、暗号化されたマスターキーまたは暗号化されたメディアキーは、制御部４３０１の制御の下、記録媒体Ｉ／Ｆ４３０３を介して記録媒体に記録される。なお、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）についても記録する。

【０３７３】なお、スタンパーＩＤ等の秘密情報は、前述の［秘密情報の書き込みおよび再生］欄で説明した例えば図２５，図２７等の構成を持つ秘密情報生成処理手段に従って生成されたデータであり、各構成に従って、スタンパーＩＤ等の秘密情報についてのデータ変換がなされ、その結果として得られる変換データが記録媒体に書き込まれる。

【０３７４】また、ディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling KeyBlock）および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、上述したようにメモリ４３０２にあらかじめ格納されているものを使用するだけでなく、たとえば入出力Ｉ／Ｆ４３０４を介して鍵発行センタから送られてきたものを入手することも可能である。

【０３７５】図４８には、本発明の記録媒体製造方法として、上記記録媒体を製造すると共に、記録媒体に対してディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する記録媒体製造方法における製造工程の流れを示す。

【０３７６】図４８において、記録媒体製造方法では、まず、ステップＳ４４０１の製造工程として、図示しない公知の組立工程によりＤＶＤ、ＣＤ等各種記録媒体が組み立てられる。

【０３７７】次に、ステップＳ４４０２の製造工程として、図４７の記録媒体製造装置により、製造された記録媒体に対して、ディスクＩＤ（Disk ID），秘密情報としてのスタンパーＩＤ(Stamper ID),有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する。

【０３７８】以上のディスク製造処理プロセスにより、記録媒体は、ディスクＩＤ（Disk ID），有効化キーブロック：ＥＫＢ（Enabling Key Block）および、暗号化されたマスターキーまたは暗号化されたメディアキー、および秘密情報としてのスタンパーＩＤを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録した後、製造工場から出荷される。

【０３７９】なお、秘密情報として記録するのはスタンパーＩＤに限らず、ディスク毎に異なって設定されるディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として記録してもよい。記録再生装置においては、これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【０３８０】［ＥＫＢのフォーマット］図４９に有効化キーブロック（ＥＫＢ：Enabling Key Block）のフォーマット例を示す。バージョン４５０１は、有効化キーブロック（ＥＫＢ：Enabling KeyBlock）のバージョンを示す識別子である。デプス４５０２は、有効化キーブロック（ＥＫＢ：Enabling Key Block）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ４５０３は、有効化キーブロック（ＥＫＢ：Enabling Key Block）中のデータ部の位置を示すポインタであり、タグポインタ４５０４はタグ部の位置、署名ポインタ４５０５は署名の位置を示すポインタである。データ部４５０６は、例えば更新するノードキーを暗号化したデータを格納する。

【０３８１】タグ部４５０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図５０を用いて説明する。図５０では、データとして先に図１２（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図５０の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。

【０３８２】暗号化キーの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図５０の左の階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが

０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図５０（ｃ）に示すデータ列、およびタグ列が構成される。

【０３８３】ツリーのノード処理の順番として、同一段の幅方向を先に処理する幅優先（breadth first）処理と、深さ方向を先に処理する深さ優先（depth first）処理のいずれかを用いるのが好適である。

【０３８４】図４９に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【０３８５】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。例えば、前述したように、実施例においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーＩＤとした例を説明したが、スタンパーＩＤに限らず、ディスク毎に異なって設定されるディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。実施例においては、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０３８６】

【発明の効果】上述したように、本発明の構成においては、記録媒体に、あらかじめその書き込み／読出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報の信号を格納し、この記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記の秘密情報を作用させる構成とした。従って、特定の読み取り方法を実行可能な正当デバイスにおいてのみ、秘密情報の読み取り、コンテンツの暗号処理鍵の生成が可能となり、秘密情報の読み取り方法の実行できないデバイスにおけるコンテンツ再生を効果的に防止することが可能となる。

【０３８７】また、本発明の構成においては、特殊の読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばＬＳＩ内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【０３８８】また、本発明の構成によれば、ツリー（木）構造の鍵配布構成により、マスターキーやメディアキーの更新データを有効化キーブロック（ＥＫＢ）とともに送信し、送信したマスターキーやメディアキーと、特殊な読み取り手法でのみ読み取り可能な秘密情報とに基づいてコンテンツ暗号化あるいは復号処理用暗号鍵生成処理を実行する構成としたので、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。

【図面の簡単な説明】

【図１】本発明の情報記録再生装置の構成例（その１）を示すブロック図である。

【図２】本発明の情報記録再生装置の構成例（その２）を示すブロック図である。

【図３】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図４】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図５】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図６】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図７】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図８】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図９】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図１０】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図１１】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図１２】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図１３】本発明の情報記録再生装置におけるマスターキーの有効化キーブロック（ＥＫＢ）を使用した配布例

と復号処理例を示す図である。
【図１４】本発明の情報記録再生装置におけるマスターキーの有効化キーブロック（ＥＫＢ）を使用した復号処理フローを示す図である。
【図１５】本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。
【図１６】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図（その１）である。
【図１７】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図（その２）である。
【図１８】本発明の情報記録再生装置において、データ記録処理を説明するフローチャートである。
【図１９】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。
【図２０】本発明の情報記録再生装置において処理される伝送１３９４パケットにおけるＥＭＩ格納位置（５ＣＤＴＣＰ規格）を示す図である。
【図２１】本発明の情報記録再生装置におけるコンテンツ記録をデータ解析記録方式（Cognizant Mode)によって実行するか、データ非解析記録方式（Non-Cognizant Mode)で実行するかを決定するプロセスを説明するフロー図である。
【図２２】本発明の情報記録再生装置において、データ記録時のタイトル固有キーの生成処理例を示す図である。
【図２３】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。
【図２４】本発明の情報記録再生装置におけるタイトル固有キーの生成処理フローを示す図である。
【図２５】本発明の情報記録再生装置におけるスタンパーＩＤ等の秘密情報の記録処理に適用される変調回路を示す図である。
【図２６】図２５に示すスタンパーＩＤ等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。
【図２７】本発明の情報記録再生装置におけるスタンパーＩＤ等の秘密情報の記録構成例を示す図である。
【図２８】図２７に示すスタンパーＩＤ等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。
【図２９】本発明の情報記録再生装置におけるデータ解析記録用キーのみを格納した記録再生装置構成例を示す図である。
【図３０】本発明の情報記録再生装置におけるデータ非解析記録用キーのみを格納した記録再生装置構成例を示す図である。
【図３１】本発明の情報記録再生装置において、データ再生処理時のコンテンツデータ復号処理を説明するブロック図である。
【図３２】本発明の情報記録再生装置において、データ再生処理を説明するフローチャートである。
【図３３】本発明の情報記録再生装置において、データ再生処理における再生可能制判定処理の詳細を示すフローチャートである。
【図３４】本発明の情報記録再生装置において、データ再生時のタイトル固有キーの生成処理フローを示す図である。
【図３５】本発明の情報記録再生装置におけるメディアキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。
【図３６】本発明の情報記録再生装置におけるメディアキーの有効化キーブロック（ＥＫＢ）を使用した復号処理フローを示す図である。
【図３７】本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。
【図３８】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その１）である。
【図３９】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その２）である。
【図４０】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理を説明するフローチャートである。
【図４１】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。
【図４２】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理を説明するフローチャートである。
【図４３】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。
【図４４】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。
【図４５】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。
【図４６】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。
【図４７】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。
【図４８】本発明の情報記録再生装置において使用され

る情報記録媒体を製造する製造処理の処理フローを示す図である。

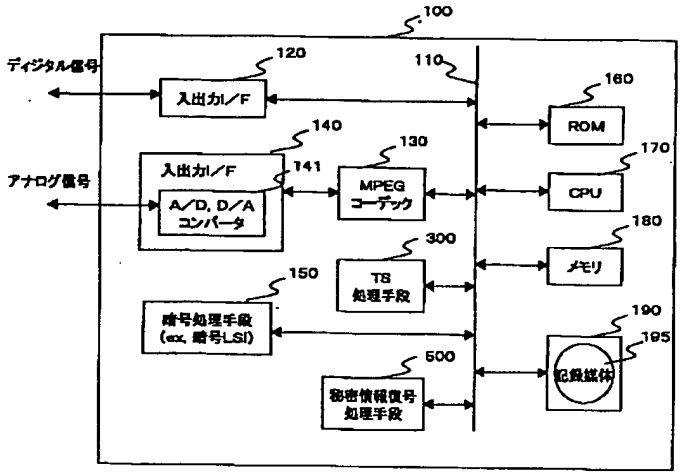
【図４９】本発明の情報記録再生装置において使用される有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

【図５０】本発明の情報記録再生装置において使用される有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

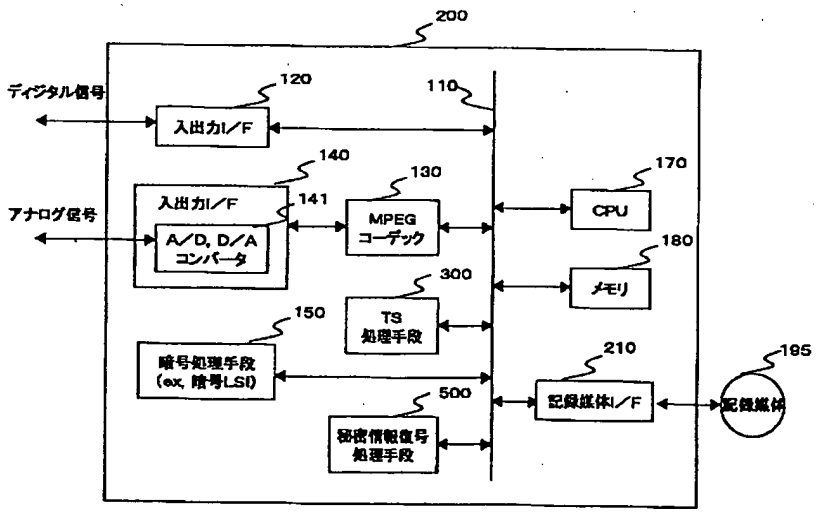
【符号の説明】

１００，２００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　ドライブ
１９５　記録媒体
２１０　記録媒体Ｉ／Ｆ
３００　ＴＳ処理手段
５００　秘密情報復号処理手段
６００，６０７　端子
６０２　ビットストリームパーサー
６０３　ＰＬＬ
６０４　タイムスタンプ発生回路
６０５　ブロックシード付加回路
６０６　スムージングバッファ
８００，８０６　端子
８０１　ブロックシード分離回路
８０２　出力制御回路
８０３　比較器
８０４　タイミング発生回路
８０５　２７ＭＨｚクロック
９０１，９０４，９１３　端子
９０２　ＭＰＥＧビデオエンコーダ
９０３　ビデオストリームバッファ
９０５　ＭＰＥＧオーディオエンコーダ
９０６　オーディオストリームバッファ
９０８　多重化スケジューラ
９０９　トランスポートパケット符号化器
９１０　到着タイムスタンプ計算手段
９１１　ブロックシード付加回路
９１２　スムージングバッファ
９７６　スイッチ
１０４１　ＰＬＬ回路
１０４２　タイミングジェネレータ
１０４３　同期パターン発生回路
１０４５　Ｍ系列発生回路
１０４６　演算回路
１０４７　乱数発生回路
１０４８　データセレクタ
１０４９　データセレクタ
１０８１　ＰＬＬ回路
１０８２　同期検出回路
１０８３　Ｍ系列発生回路
１０８４　乗算回路
１０８５　積分回路
１０８６　判定回路
１１６０　ＰＬＬ回路
１１６１　同期検出回路
１１６２　タイミングジェネレータ
１１６３　フリップフロップ
１１６４　最大値検出回路
１１６５　パラレルシリアル変換回路
４２０２　ＣＰＵ
４２０３　ＲＯＭ
４２０４　ＲＡＭ
４２０５　ハードディスク
４２０６　出力部
４２０７　入力部
４２０８　通信部
４２０９　ドライブ
４２１０　リムーバブル記録媒体
４２１１　入出力インタフェース
４３００　ディスク製造装置
４３０１　制御部
４３０２　メモリ
４３０３　記録媒体Ｉ／Ｆ
４３０４　入出力Ｉ／Ｆ
４３０５　バス
４３５０　記録媒体
４５０１　バージョン
４５０２　デプス
４５０３　データポインタ
４５０４　タグポインタ
４５０５　署名ポインタ
４５０６　データ部
４５０７　タグ部
４５０８　署名

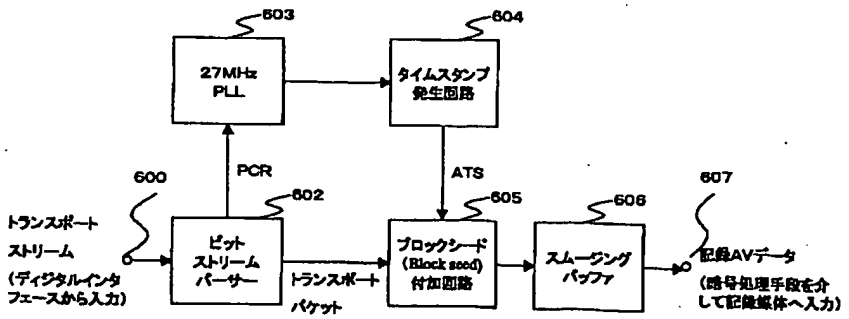
【図１】


100
ディジタル信号
120
入出力I／F
110
160
ROM
140
入出力I／F
141
A／D, D／A
コンバータ
130
MPEG
コーデック
170
CPU
アナログ信号
180
メモリ
300
TS
処理手段
150
暗号処理手段
(ex, 暗号LSI)
190
195
記録媒体
500
秘密情報復号
処理手段

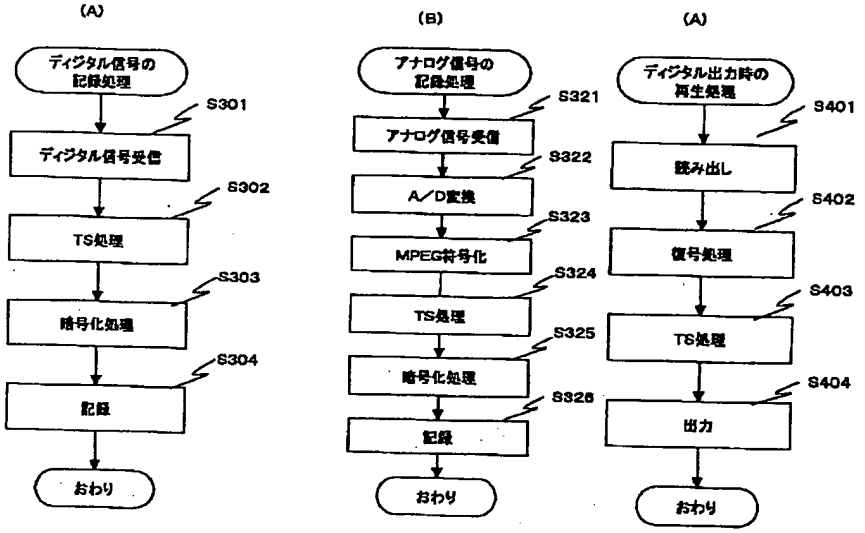
【図２】


200
ディジタル信号
120
入出力I／F
110
140
入出力I／F
141
A／D, D／A
コンバータ
130
MPEG
コーデック
170
CPU
アナログ信号
180
メモリ
300
TS
処理手段
150
暗号処理手段
(ex, 暗号LSI)
210
195
記録媒体I／F
記録媒体
500
秘密情報復号
処理手段

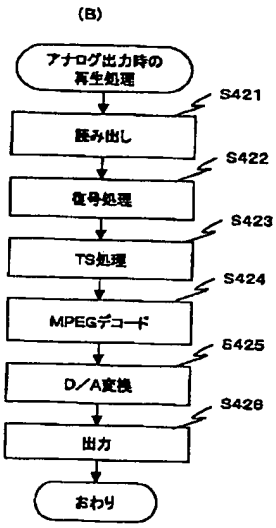
【図６】


603
27MHz
PLL
604
タイムスタンプ
発生回路
PCR
ATS
600
602
605
606
607
トランスポート
ストリーム
(ディジタルインタ
フェースから入力)
ビット
ストリーム
パーサー
トランスポート
パケット
ブロックシード
(Block seed)
付加回路
スムージング
バッファ
記録AVデータ
(暗号処理手段を介
して記録媒体へ入力)

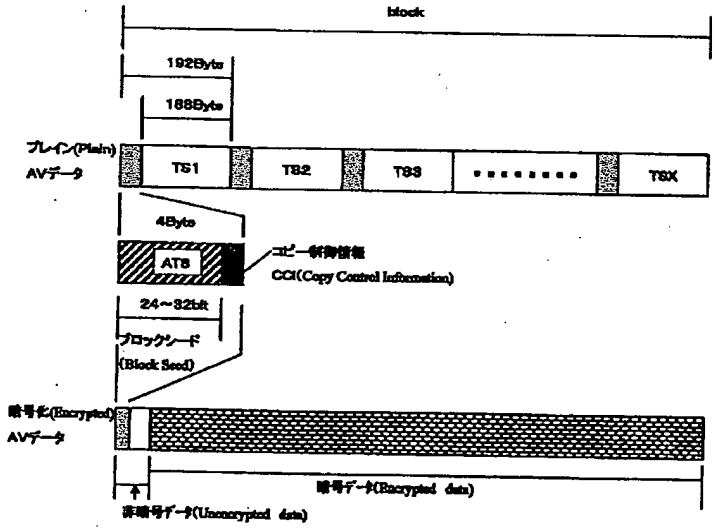
【図３】



【図４】



【図５】



【図１２】

(A) キー更新ブロック(KRB:Key Renewal Block)　例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

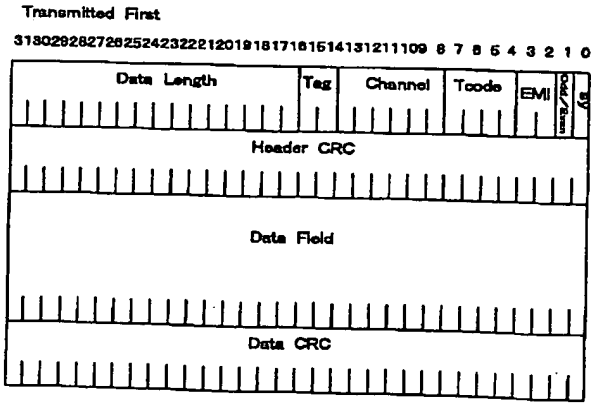
世代(Generation):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB:Key Renewal Block)　例2

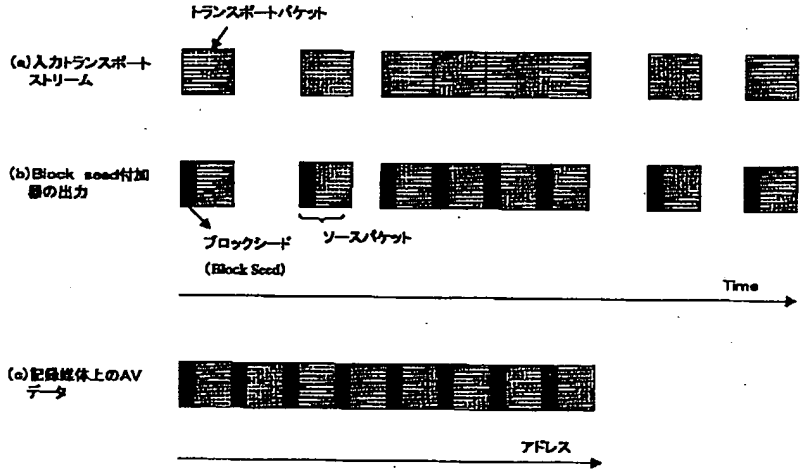
デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generation):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

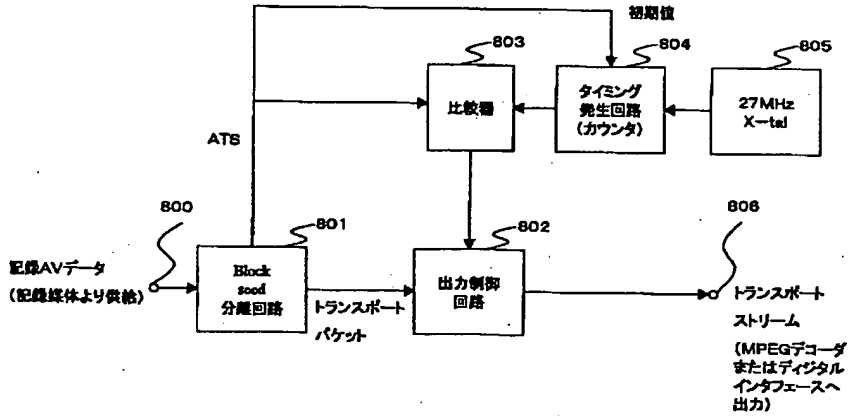
【図２０】



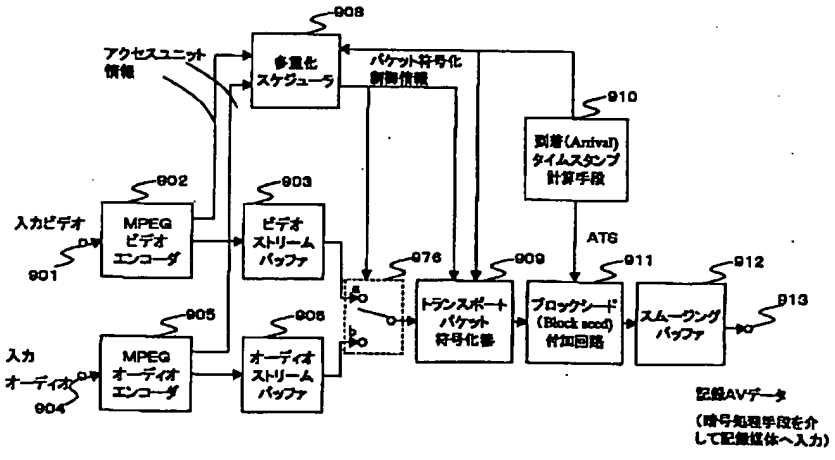
【図７】


トランスポートパケット
(a)入力トランスポートストリーム
(b)Block seed付加器の出力
ブロックシード
(Block Seed)
ソースパケット
Time
(c)記録媒体上のAVデータ
アドレス

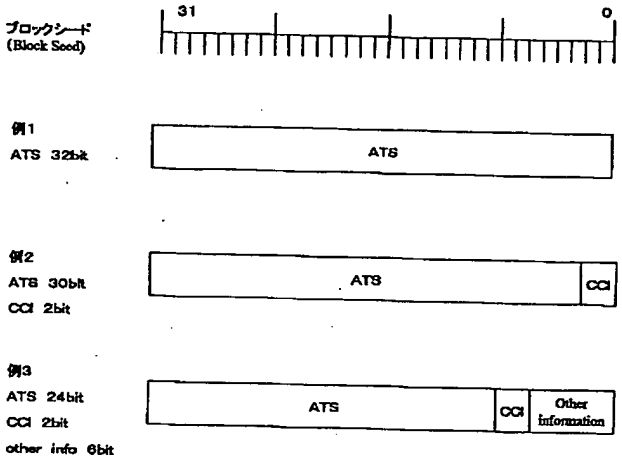
【図８】


初期値
803
804
805
比較器
タイミング発生回路(カウンタ)
27MHz X-tal
ATS
800
801
802
806
記録AVデータ
(記録媒体より供給)
Block seed 分離回路
トランスポートパケット
出力制御回路
トランスポートストリーム
(MPEGデコーダまたはディジタルインタフェースへ出力)

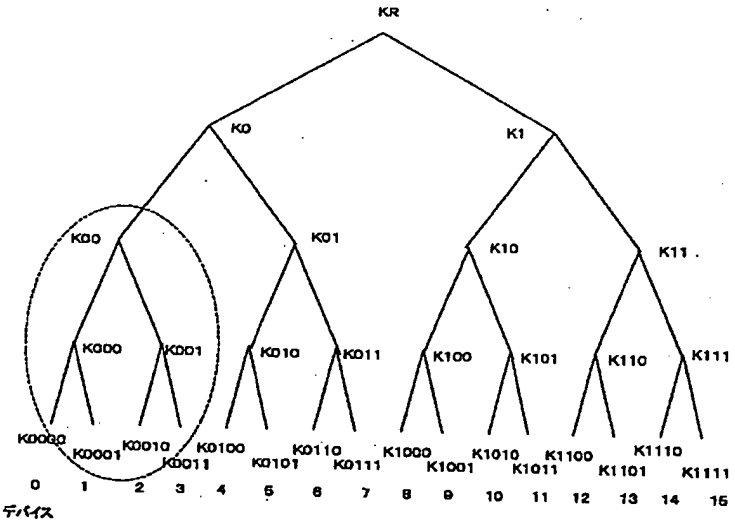
【図９】


908
アクセスユニット情報
多重化スケジューラ
パケット符号化制御情報
910
到着(Arrival)タイムスタンプ計算手段
902
903
入力ビデオ
901
MPEG ビデオエンコーダ
ビデオストリームバッファ
976
909
911
912
913
ATS
905
906
入力オーディオ
904
MPEG オーディオエンコーダ
オーディオストリームバッファ
トランスポートパケット符号化器
ブロックシード(Block seed)付加回路
スムージングバッファ
記録AVデータ
(暗号処理手段を介して記録媒体へ入力)

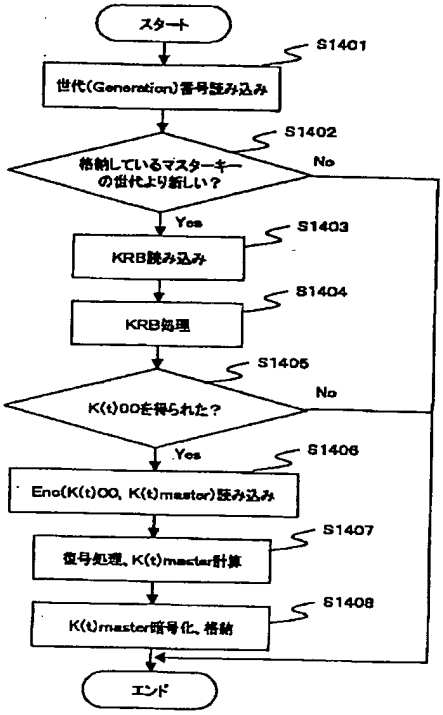
【図１０】



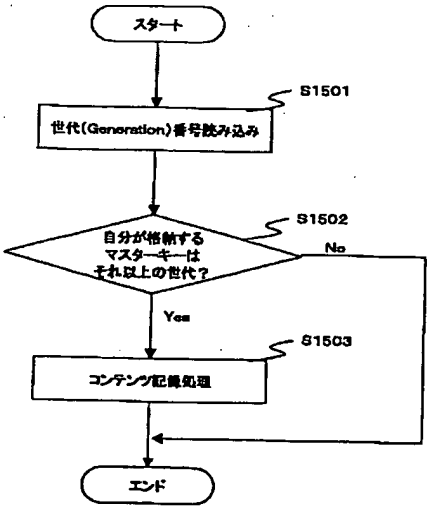
【図１１】



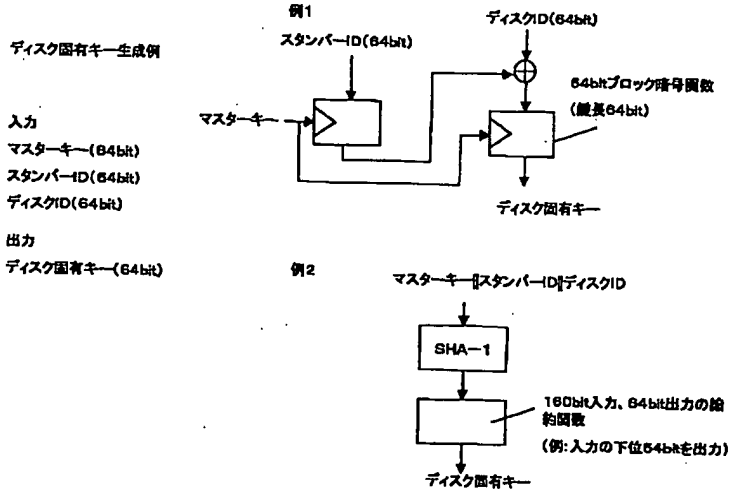
【図１４】



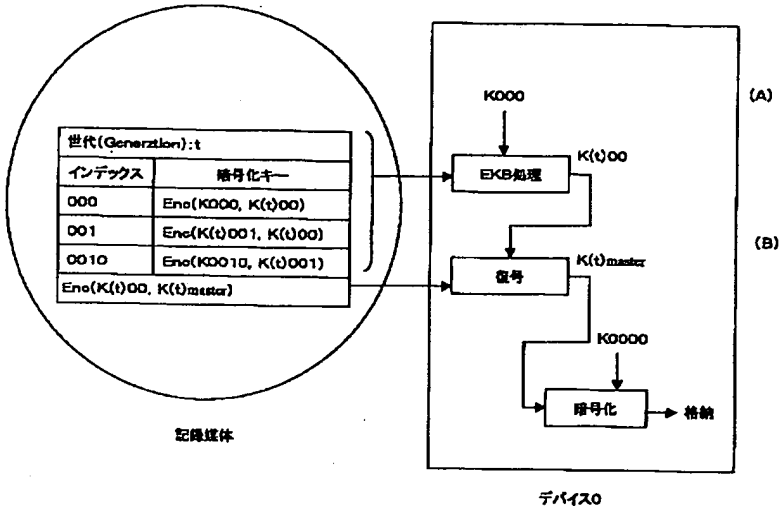
【図１５】



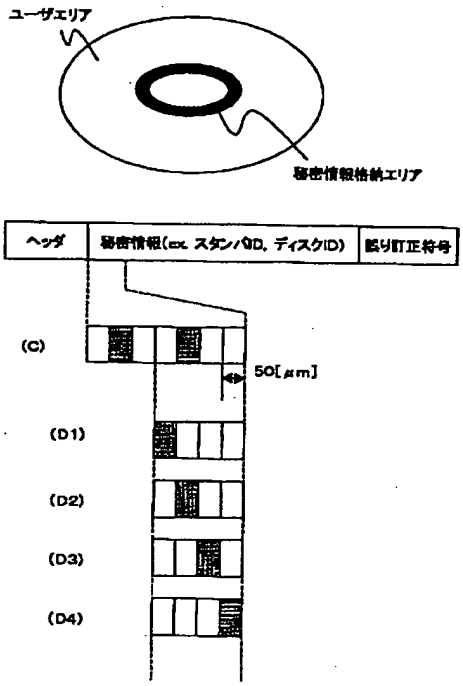
【図１９】



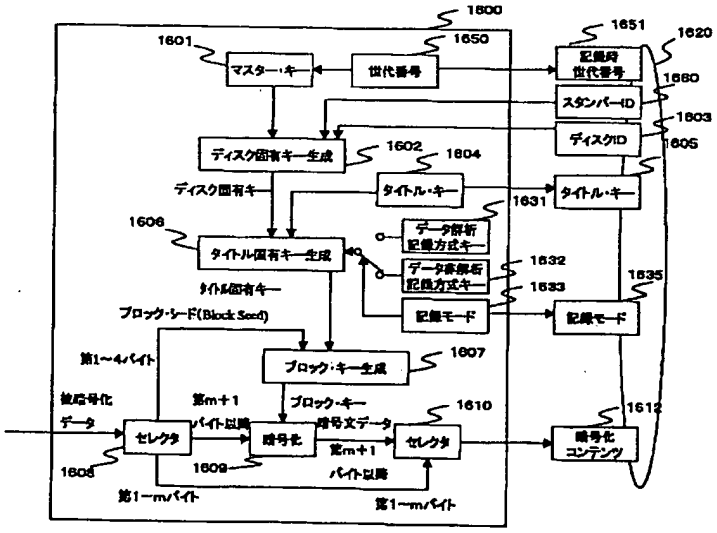
【図１３】



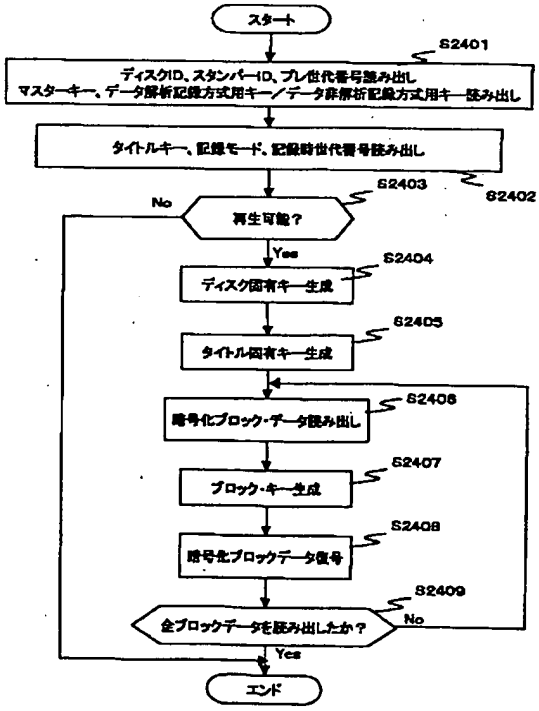
【図２７】



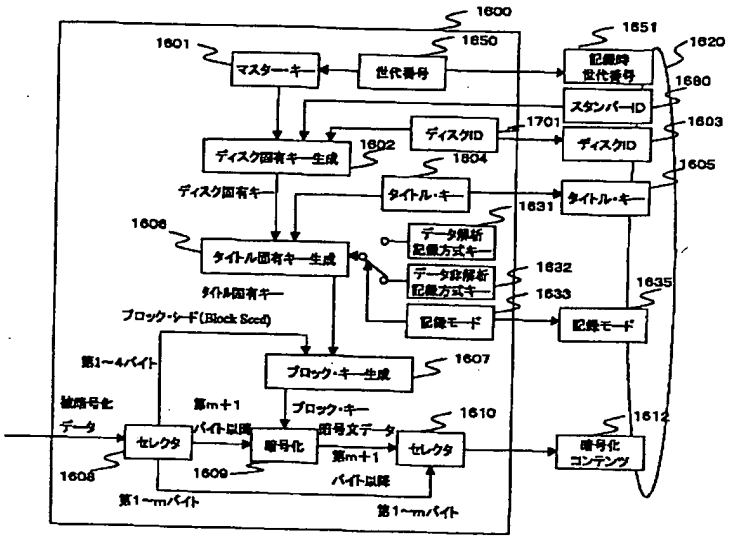
【図１６】



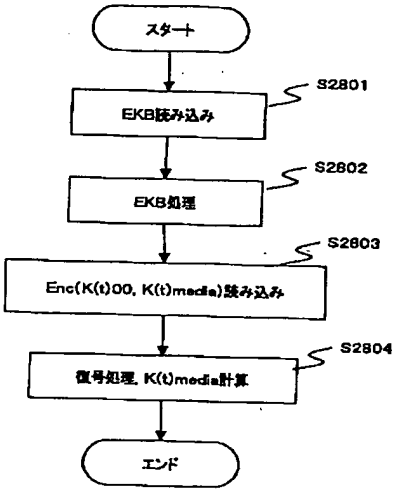
【図３２】



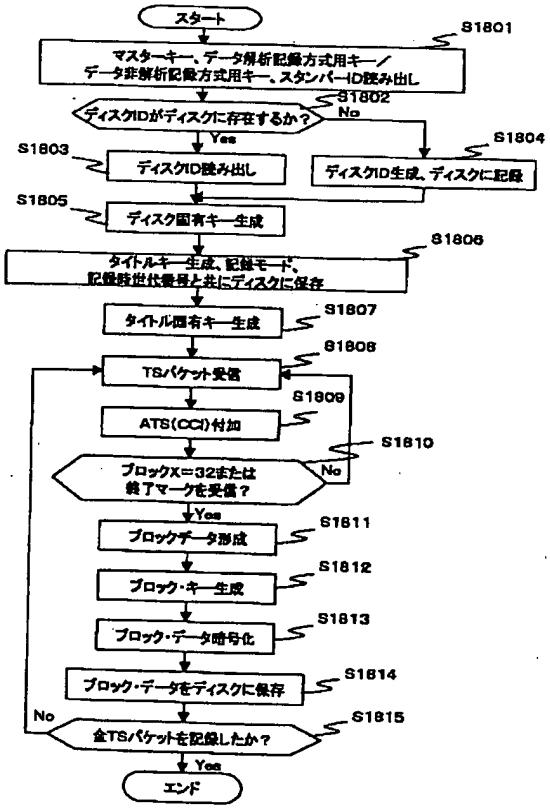
【図１７】



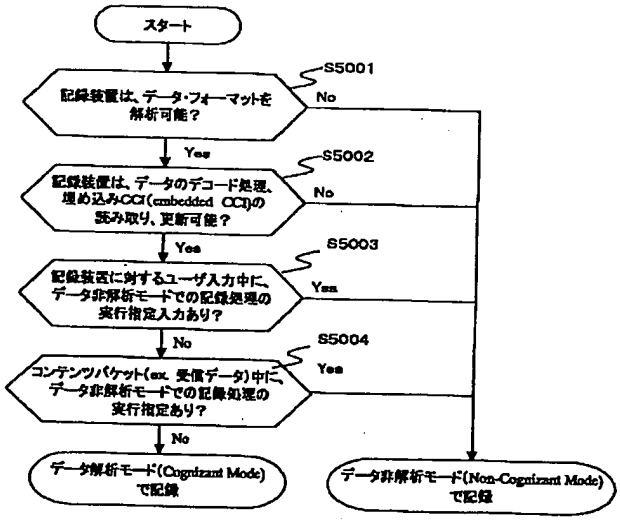
【図３６】



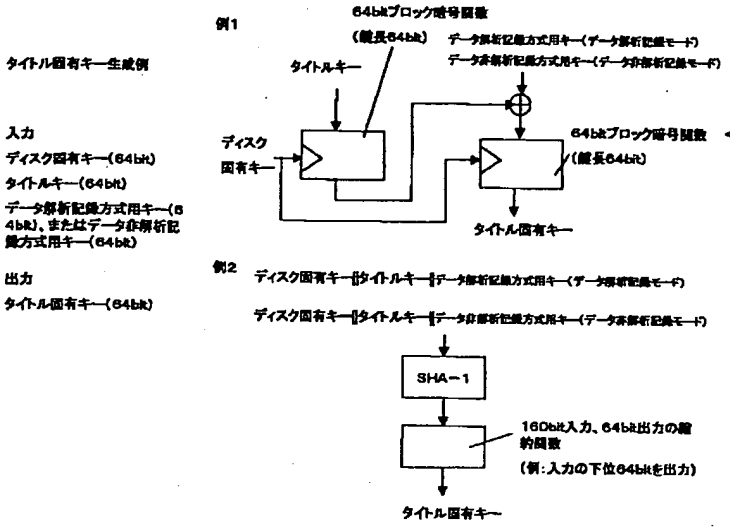
【図１８】



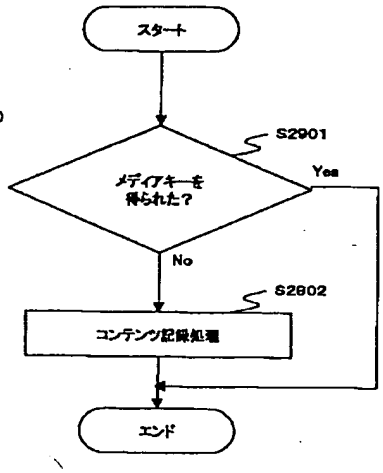
【図２１】



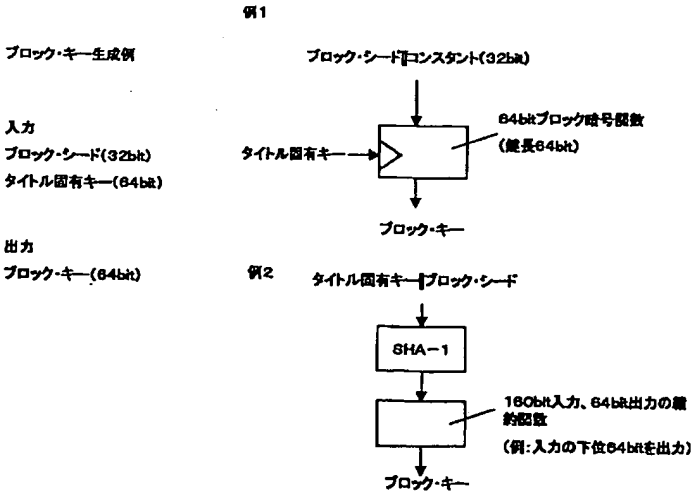
【図２２】



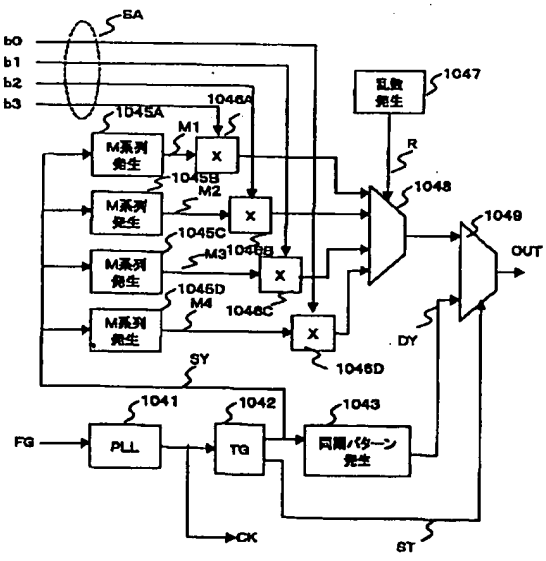
【図３７】



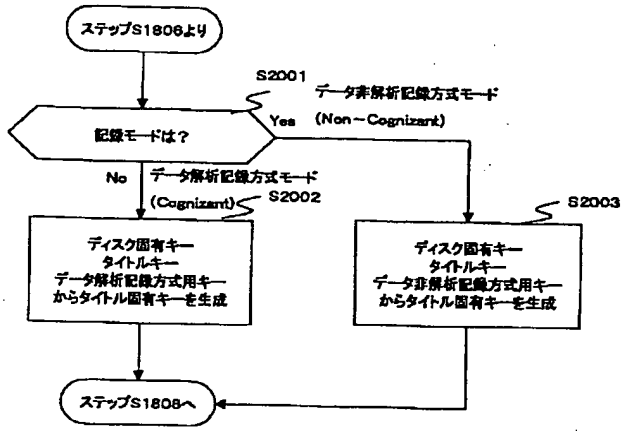
【図２３】



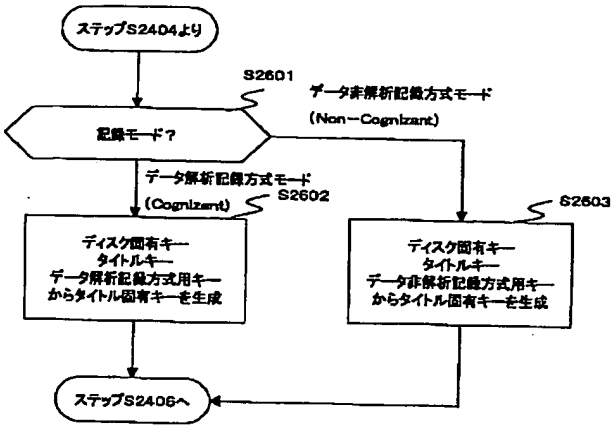
【図２５】



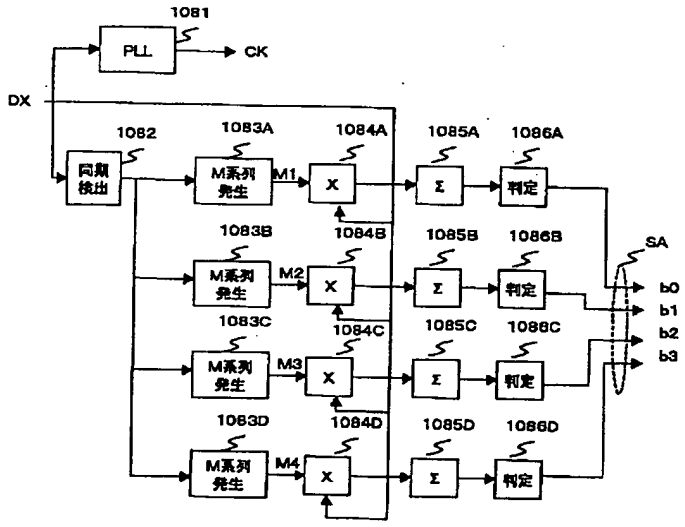
【図２４】



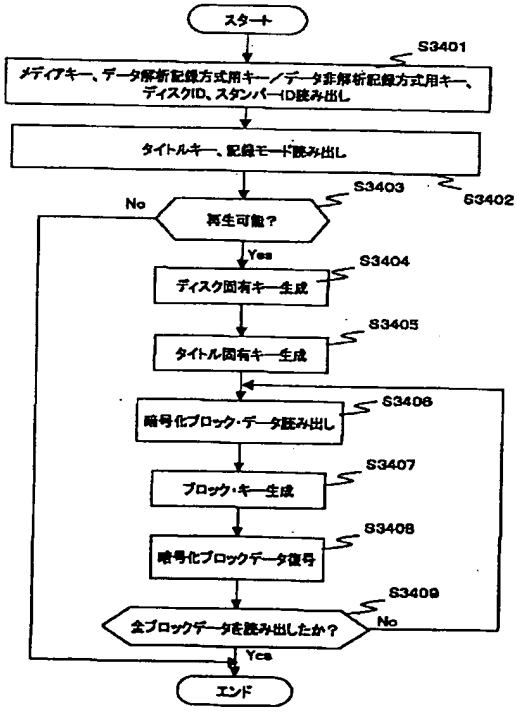
【図３４】



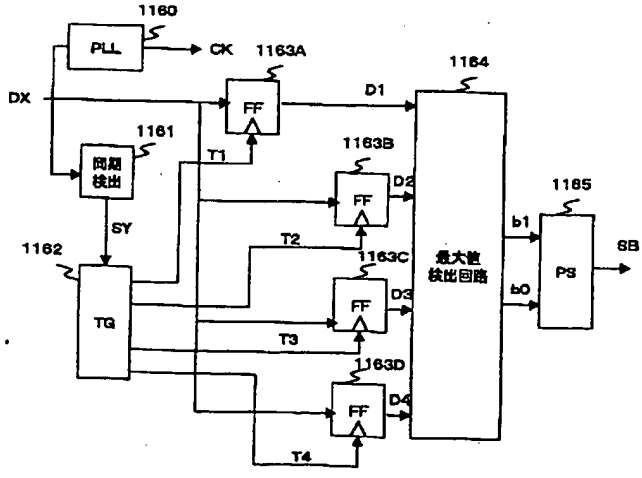
【図２６】



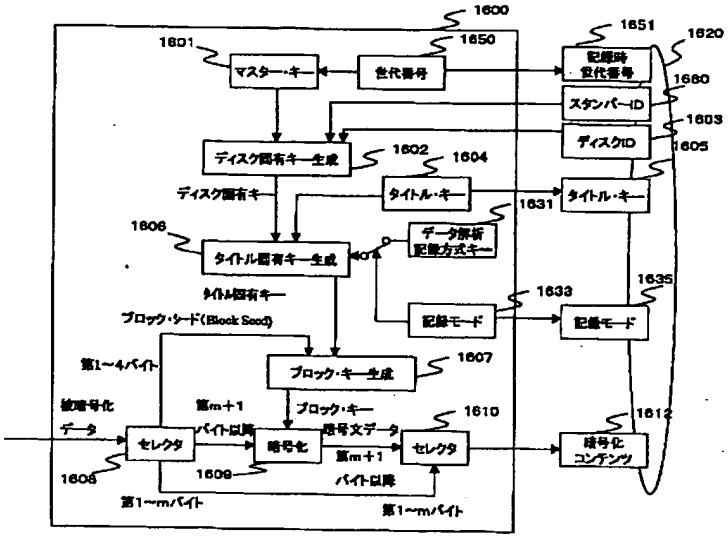
【図４２】



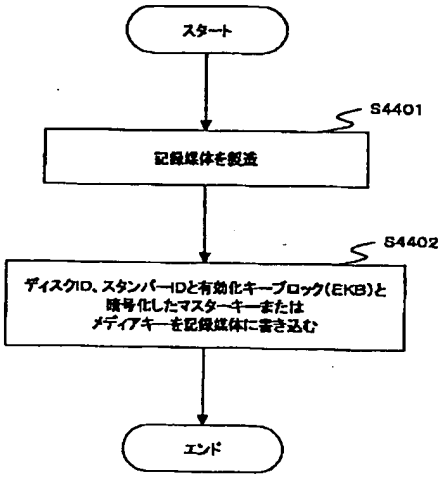
【図２８】



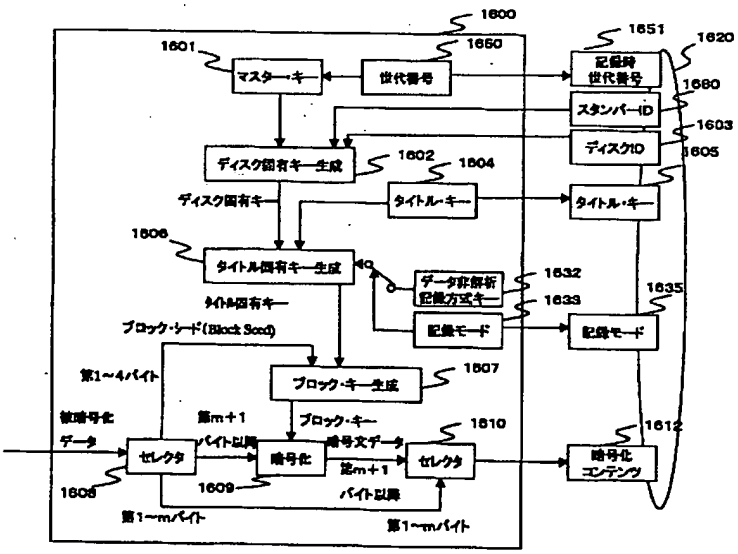
【図２９】


1600
1601
マスター・キー
1650
世代番号
1651
記録時世代番号
1620
1660
スタンバーID
1603
ディスクID
1605
ディスク固有キー生成
1602
1604
ディスク固有キー
タイトル・キー
タイトル・キー
1631
1606
タイトル固有キー生成
40
データ解析記録方式キー
タイトル固有キー
1635
1633
ブロック・シード(Block Seed)
記録モード
記録モード
第1～4バイト
ブロック・キー生成
1607
被暗号化データ
第m＋1バイト以降
ブロック・キー
暗号文データ
1610
1612
セレクタ
暗号化
第m＋1バイト以降
セレクタ
暗号化コンテンツ
1608
1609
第1～mバイト
第1～mバイト

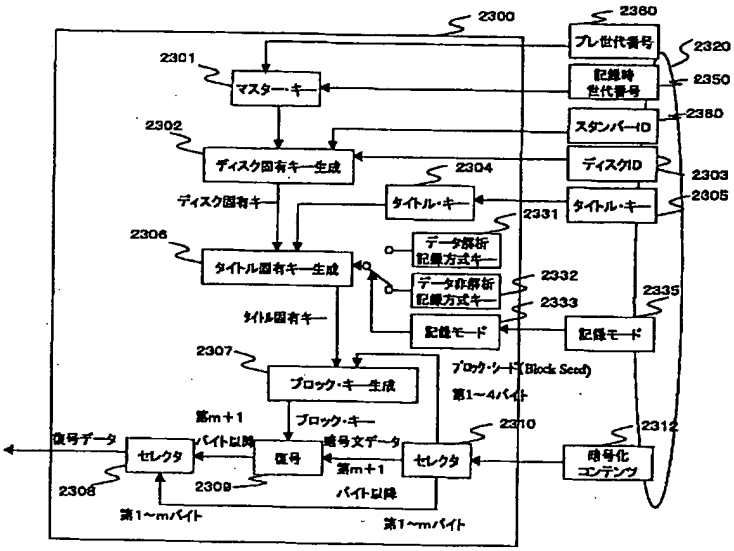
【図４８】


スタート
S4401
記録媒体を製造
S4402
ディスクID、スタンバーIDと有効化キーブロック(EKB)と
暗号化したマスターキーまたは
メディアキーを記録媒体に書き込む
エンド

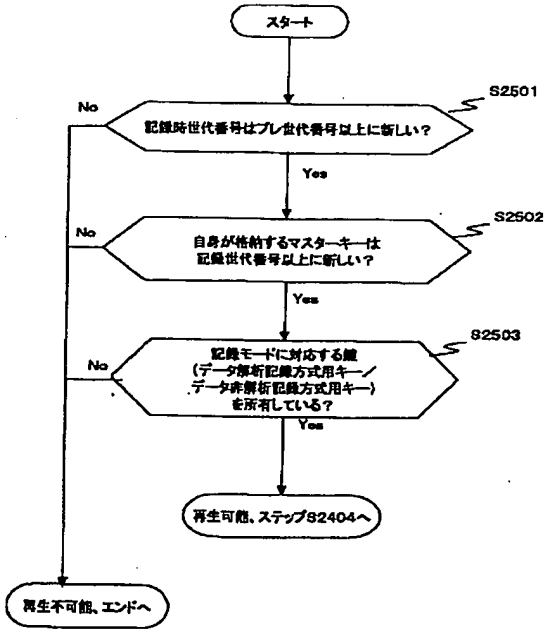
【図３０】


1600
1601
マスター・キー
1650
世代番号
1651
記録時世代番号
1620
1660
スタンバーID
1603
ディスクID
1605
ディスク固有キー生成
1602
1604
ディスク固有キー
タイトル・キー
タイトル・キー
1606
タイトル固有キー生成
40
データ非解析記録方式キー
1632
1633
1635
タイトル固有キー
ブロック・シード(Block Seed)
記録モード
記録モード
第1～4バイト
ブロック・キー生成
1607
被暗号化データ
第m＋1バイト以降
ブロック・キー
暗号文データ
1610
1612
セレクタ
暗号化
第m＋1バイト以降
セレクタ
暗号化コンテンツ
1608
1609
第1～mバイト
第1～mバイト

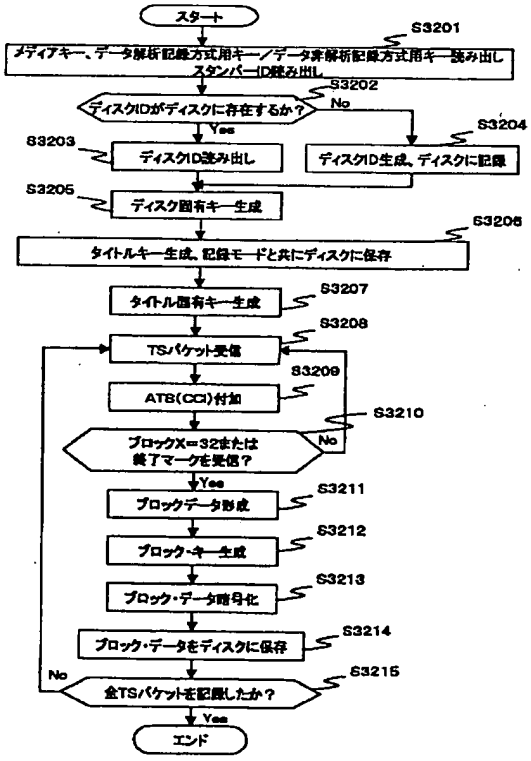
【図３１】


2300
2360
プレ世代番号
2320
2301
マスター・キー
記録時世代番号
2350
2302
スタンバーID
2380
ディスク固有キー生成
ディスクID
2303
2304
ディスク固有キー
タイトル・キー
タイトル・キー
2305
2331
2306
データ解析記録方式キー
タイトル固有キー生成
データ非解析記録方式キー
2332
2335
2333
タイトル固有キー
記録モード
記録モード
2307
ブロック・キー生成
ブロック・シード(Block Seed)
第1～4バイト
第m＋1バイト以降
ブロック・キー
2310
2312
復号データ
セレクタ
復号
暗号文データ
セレクタ
暗号化コンテンツ
第m＋1バイト以降
2308
2309
第1～mバイト
第1～mバイト

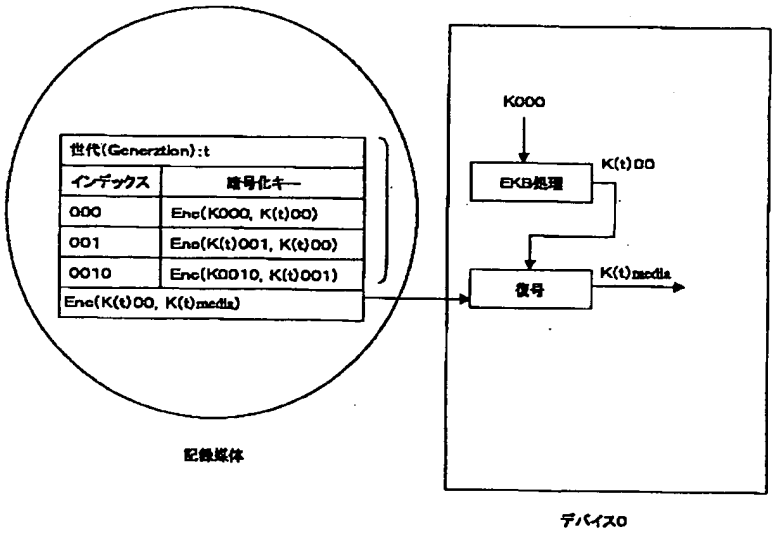
【図３３】


スタート
S2501
No
記録時世代番号はプレ世代番号以上に新しい？
Yes
S2502
No
自身が性能するマスターキーは記録世代番号以上に新しい？
Yes
S2503
No
記録モードに対応する鍵(データ解析記録方式用キー／データ非解析記録方式用キー)を所有している？
Yes
再生可能、ステップS2404へ
再生不可能、エンドへ

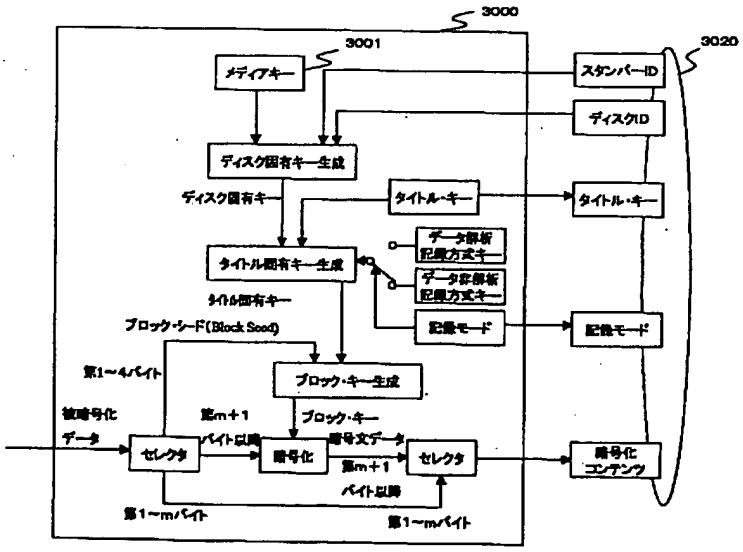
【図４０】


スタート
S3201
メディアキー、データ解析記録方式用キー／データ非解析記録方式用キー読み出し
スタンバーID読み出し
S3202
ディスクIDがディスクに存在するか？
No
Yes
S3204
S3203
ディスクID読み出し
ディスクID生成、ディスクに記録
S3205
ディスク固有キー生成
S3206
タイトルキー生成、記録モードと共にディスクに保存
S3207
タイトル固有キー生成
S3208
TSパケット受信
S3209
ATB(CCI)付加
S3210
ブロックX＝32または終了マークを受信？
No
Yes
S3211
ブロックデータ形成
S3212
ブロック・キー生成
S3213
ブロック・データ暗号化
S3214
ブロック・データをディスクに保存
S3215
No
全TSパケットを記録したか？
Yes
エンド

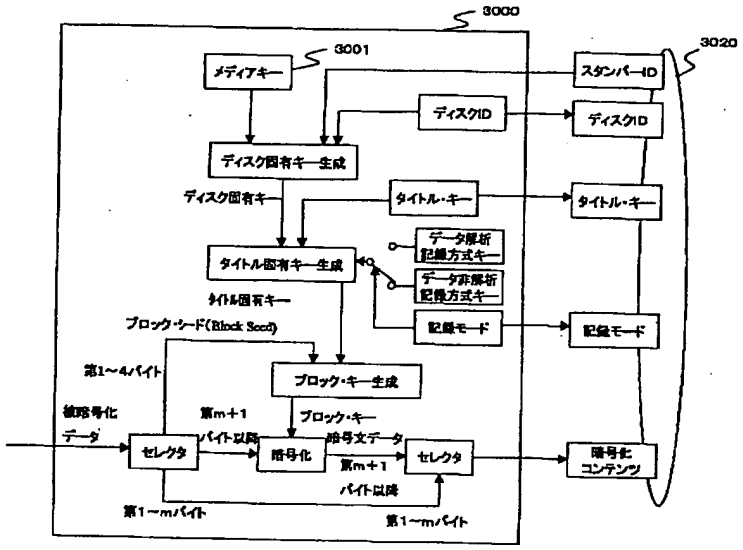
【図３５】


世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
記録媒体
K000
EKB処理
K(t)00
復号
K(t)media
デバイス0

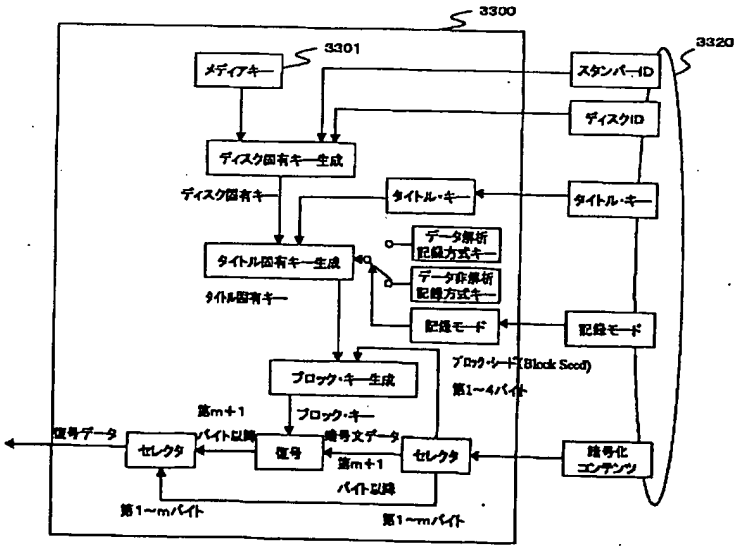
【図３８】


3000
3001
3020
メディアキー
スタンパーID
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
データ鍵情報記録方式キー
タイトル固有キー生成
データ非鍵情報記録方式キー
タイトル固有キー
記録モード
記録モード
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー生成
被暗号化データ
第m+1バイト以降
ブロック・キー
セレクタ
暗号化
暗号文データ
第m+1バイト以降
セレクタ
暗号化コンテンツ
第1～mバイト
第1～mバイト

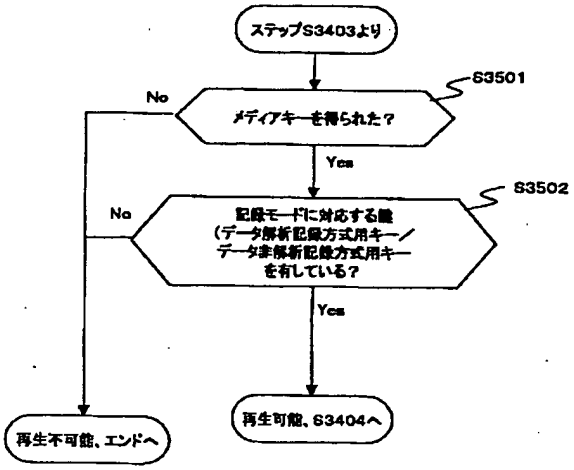
【図３９】


3000
3001
3020
メディアキー
スタンパーID
ディスクID
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
データ解析記録方式キー
タイトル固有キー生成
データ非解析記録方式キー
タイトル固有キー
ブロック・シード(Block Seed)
記録モード
記録モード
第1～4バイト
ブロック・キー生成
被暗号化データ
第m＋1バイト以降
ブロック・キー
セレクタ
暗号化
暗号文データ
第m＋1バイト以降
セレクタ
暗号化コンテンツ
第1～mバイト
第1～mバイト

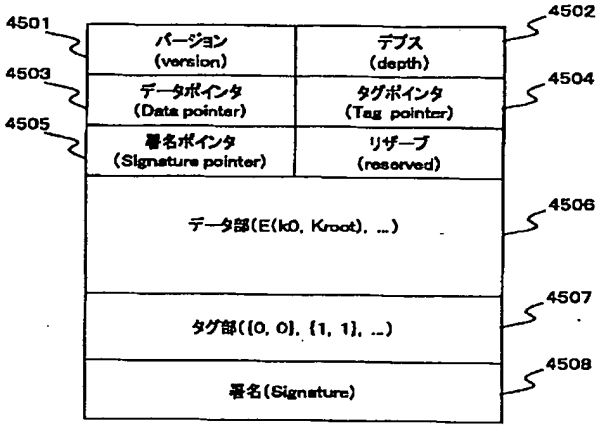
【図４１】


3300
3301
3320
メディアキー
スタンパーID
ディスクID
ディスク固有キー生成
ディスク固有キー
タイトル・キー
タイトル・キー
データ解析記録方式キー
タイトル固有キー生成
データ非解析記録方式キー
タイトル固有キー
記録モード
記録モード
ブロック・シード(Block Seed)
ブロック・キー生成
第1～4バイト
第m＋1バイト以降
ブロック・キー
復号データ
セレクタ
復号
暗号文データ
セレクタ
暗号化コンテンツ
第m＋1バイト以降
第1～mバイト
第1～mバイト

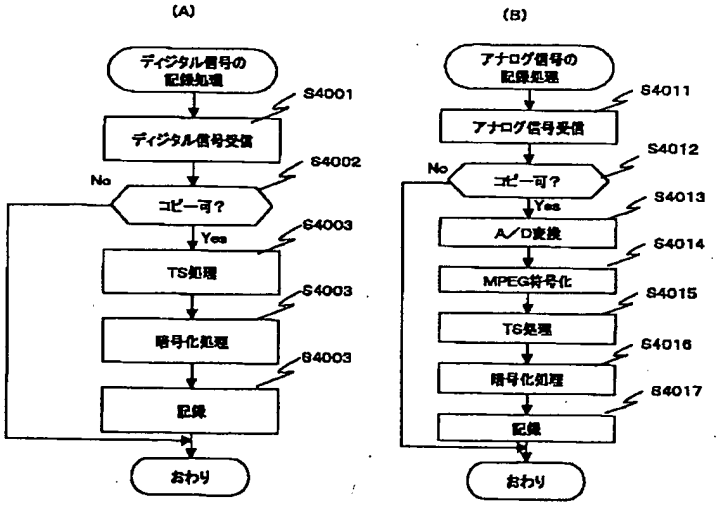
【図４３】



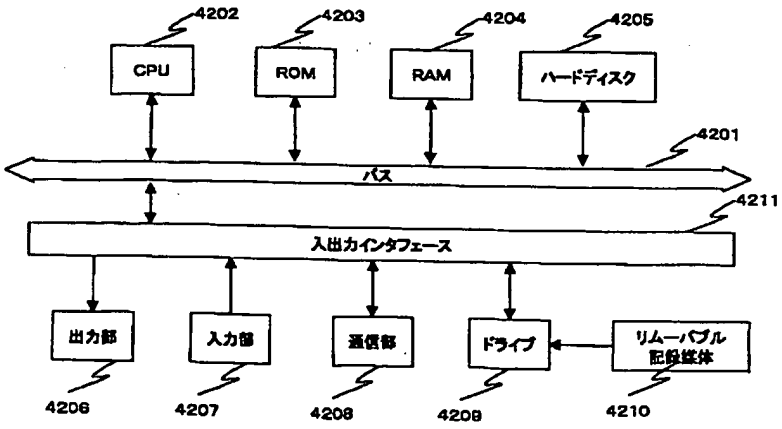
【図４９】



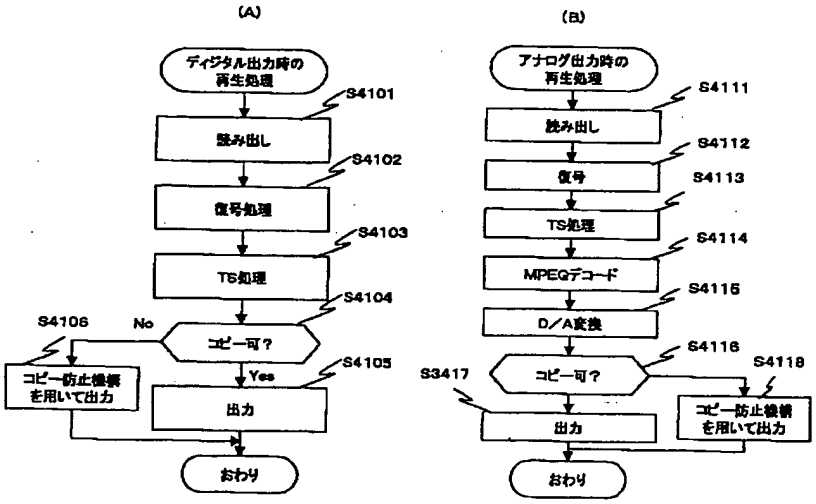
【図４４】



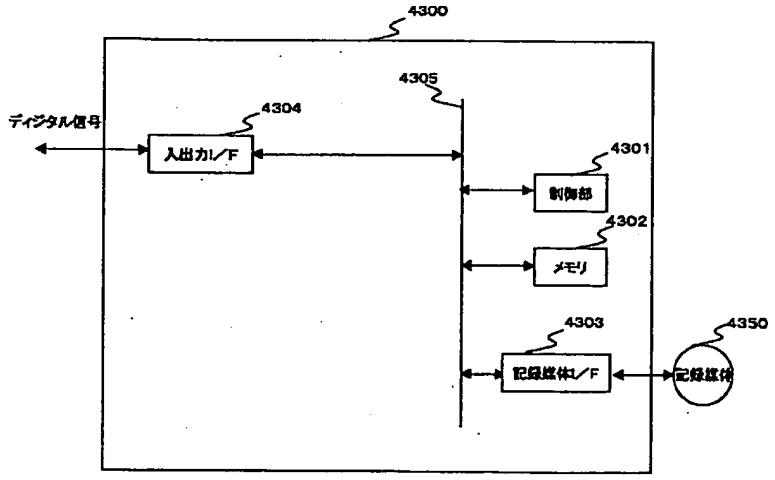
【図４６】



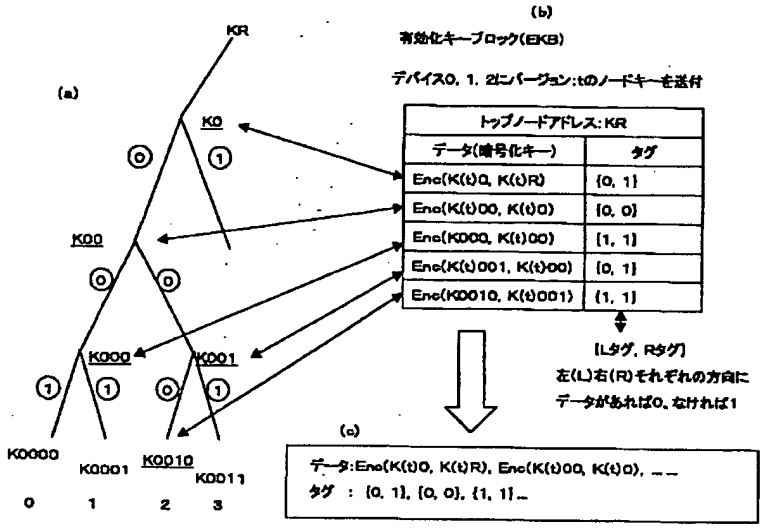
【図４５】


(A)
ディジタル出力時の再生処理
S4101
読み出し
S4102
復号処理
S4103
TS処理
S4104
コピー可？
No
S4106
コピー防止機構を用いて出力
Yes
S4105
出力
おわり
(B)
アナログ出力時の再生処理
S4111
読み出し
S4112
復号
S4113
TS処理
S4114
MPEGデコード
S4115
D／A変換
S4116
コピー可？
S4118
コピー防止機構を用いて出力
S3417
出力
おわり

【図４７】


4300
4305
ディジタル信号
4304
入出力I／F
4301
制御部
4302
メモリ
4303
記録媒体I／F
4350
記録媒体

【図５０】



フロントページの続き

Ｆターム(参考) 5D044 AB01 AB05 AB07 BC02 CC04
EF05 FG18 GK17 HH13 HH15
HL06
5J104 AA01 AA12 AA16 EA04 EA26
JA03 MA08 NA02 NA31 NA32
PA14